**United States Government Accountability Office**
**Washington, DC 20548**

July 29, 2011

The Honorable W. “Mac” Thornberry
Chairman
The Honorable James R. Langevin
Ranking Member
Subcommittee on Emerging Threats and Capabilities
Committee on Armed Services
House of Representatives

Subject: *Defense Department Cyber Efforts: Definitions, Focal Point, and Methodology Needed for DOD to Develop Full-Spectrum Cyberspace Budget Estimates*

This letter formally transmits the enclosed final briefing in response to a request from the House Armed Services Committee, Subcommittee on Emerging Threats and Capabilities, that asked GAO to examine the Department of Defense’s (DOD) cyber and information assurance budget for fiscal year 2012 and future years defense spending. The objectives of this review were to (1) assess the extent to which DOD has prepared an overarching budget estimate for full-spectrum cyberspace operations across the department; and (2) identify the challenges DOD has faced in providing such estimates. We provided your offices a preliminary briefing on these issues on April 28, 2011.

The President has identified the cyber threat as one of the most serious national security challenges that the nation faces. In February 2011 the Deputy Secretary of Defense[1] said that more than 100 foreign intelligence agencies have tried to breach DOD computer networks, and that one was successful in breaching networks containing classified information. To aid its efforts in countering cyberspace threats, DOD established the U.S. Cyber Command in 2010 and is currently undertaking departmentwide efforts to defend against cyber threats. [2]

[1] Deputy Secretary of Defense William J. Lynn, III, Remarks on Cyber at the RSA Conference, February 15, 2011.

[2] In May 2011, we reported that DOD and U.S. Cyber Command had made progress in identifying roles and responsibilities, describing command and control relationships, and defining long-term mission requirements, but that a greater level of detail was needed to guide the military services’ efforts. GAO, *Defense Department Cyber Efforts: More Detailed Guidance Needed to Ensure Military Services Develop Appropriate Cyberspace Capabilities*, GAO-11-421 (Washington, D.C.: May 20, 2011).

| | |
|---|---|
| **Report Documentation Page** | *Form Approved*<br>*OMB No. 0704-0188* |

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

| | | |
|---|---|---|
| 1. REPORT DATE<br>**29 JUL 2011** | 2. REPORT TYPE | 3. DATES COVERED<br>**00-00-2011 to 00-00-2011** |

| | |
|---|---|
| 4. TITLE AND SUBTITLE<br>**Defense Department Cyber Efforts: Definitions, Focal Point, and Methodology Needed for DOD to Develop Full-Spectrum Cyberspace Budget Estimates** | 5a. CONTRACT NUMBER<br>5b. GRANT NUMBER<br>5c. PROGRAM ELEMENT NUMBER |
| 6. AUTHOR(S) | 5d. PROJECT NUMBER<br>5e. TASK NUMBER<br>5f. WORK UNIT NUMBER |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)<br>**U.S. Government Accountability Office,441 G Street NW,Washington,DC,20548** | 8. PERFORMING ORGANIZATION REPORT NUMBER |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSOR/MONITOR'S ACRONYM(S)<br>11. SPONSOR/MONITOR'S REPORT NUMBER(S) |

12. DISTRIBUTION/AVAILABILITY STATEMENT
**Approved for public release; distribution unlimited**

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT<br>**unclassified** | b. ABSTRACT<br>**unclassified** | c. THIS PAGE<br>**unclassified** | **Same as Report (SAR)** | **33** | |

DOD has defined some key cyber-related terms. Cyberspace operations is defined as the employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace. Such operations include computer network operations and activities to operate and defend the global information grid.[3] U.S. Cyber Command defines full-spectrum cyber operations as the employment of the full range of cyberspace operations to support combatant command operational requirements and the defense of DOD information networks. This includes efforts such as computer network defense, computer network attack, and computer network exploitation.[4] Computer network defense is defined as actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within DOD information systems and computer networks. Computer network attack is defined as actions taken to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Computer network exploitation is defined as enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks.[5] Information assurance is defined as measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.[6]

To examine DOD funding for cyberspace operations, we reviewed and analyzed various DOD cyber-related budget documents including the department's *Fiscal Year 2012 IT [Information Technology] President's Budget Request*. [7] We also reviewed Information Assurance budget figures for the DOD for fiscal years 2010-2016. Additionally we obtained and analyzed key budget documents and met with officials from key organizations, including the Office of the Secretary of Defense, Assistant Secretary of Defense for Networks and Information Integration and Chief Information Officer; Office of the Under Secretary of Defense Comptroller / Chief Financial Officer; Office of the Under Secretary of Defense for Intelligence; U.S. Cyber Command; U.S. Army; U.S. Air Force; U.S. Navy; U.S. Marine Corps; National Security Agency; and the Defense Information Systems Agency. We made a standardized request to the DOD components and military services for information regarding funding for cyberspace operations and budget estimates. We further obtained classified budget information taken from the military intelligence program

[3] DOD defines the global information grid as the globally interconnected, end-to-end set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The global information grid includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services and National Security Systems. Joint Chiefs of Staff, Joint Pub. 1-02, Department of Defense Dictionary of Military and Associated Terms (Nov. 8, 2010, as amended through May 15, 2011).

[4] Joint Chiefs of Staff, Joint Pub. 1-02.

[5] Joint Chiefs of Staff, Joint Pub. 1-02.

[6] Joint Chiefs of Staff, Joint Pub. 1-02.

[7] DOD, *Fiscal Year 2012 IT Presidents Budget Request*, (Washington, D.C., March 2011)

budget, but not from the national intelligence program. See enclosure I, slide 6, for a list of organizations we met with.

We conducted this performance audit from March to July 2011, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

## Summary

DOD has planned and budgeted for information assurance programs for fiscal year 2012 and has projected future years' spending for these programs. However, DOD does not yet have an overarching budget estimate for full-spectrum cyberspace operations including computer network attack, computer network exploitation, and classified funding. During February and March 2011, DOD provided Congress with three different views of its cybersecurity budget estimates for fiscal year 2012 ($2.3 billion, $2.8 billion, and $3.2 billion, respectively) that included different elements of DOD's cybersecurity efforts.[8] The three budget views are largely related to the Defense-wide Information Assurance Program and do not include all full-spectrum cyber operation costs, such as computer network exploitation and computer network attack, which are funded through classified programs from the national intelligence and military intelligence program budgets. In addition, according to U.S. Cyber Command officials, the command was being established as the fiscal year 2012 information assurance budget was being developed, and therefore its funding was not coded as information assurance and consequently not included in the $2.8 billion President's budget submission. However, U.S. Cyber Command officials expect that command funding will be included in the fiscal year 2013 information assurance budget.

DOD's ability to develop an overarching budget estimate for full-spectrum cyberspace operations has been challenged by the absence of clear, agreed-upon departmentwide budget definitions and program elements for full-spectrum

[8] DOD's $2.3 billion cybersecurity budget estimate, provided in February 2011, included $2.0 billion for information assurance including Information Systems Security Program (ISSP), Public Key Infrastructure (PKI) and Key Management Infrastructure (KMI), $200 million for unclassified programs in Comprehensive National Cybersecurity Initiative (CNCI) and Defense Industrial Base (DIB), and $119 million for U.S. Cyber Command operations and maintenance. DOD's $2.8 billion cybersecurity budget estimate, provided in March 2011, included $2.0 billion for information assurance including ISSP, PKI, and KMI, $276 million for unclassified and classified programs in CNCI and DIB, and $547 million for other cybersecurity and information assurance programs. However, funding for U.S. Cyber Command was not included in this estimate. DOD's $3.2 billion defensive cybersecurity budget estimate, also provided in March 2011, included the entirety of the above $2.8 billion estimate and an additional $119 million for operations, $26 million for research and development, and $15 million for military construction for the U.S. Cyber Command, $26 million for the Defense Cyber Crime Center, and $258 million for Science and Technology.

cyberspace operations and the absence of a central organization or a methodology for collecting and compiling budget information on cyberspace operations.

With regard to the first issue, DOD has defined some key cyber-related terms but it has not yet fully identified the specific types of operations and program elements that are associated with full-spectrum cyberspace operations for budgeting purposes. In the absence of such definitions, there are differing perspectives on the elements that constitute cyberspace operations in DOD. DOD's *Financial Management Regulation* established steps for budget submission requirements and for reporting information technology and information assurance programs to Congress, including identifying the activities that constitute information assurance.[9] Although computer network defense is included in the list of information assurance activities, computer network attack and computer network exploitation, which are part of full-spectrum cyberspace operations, are not accounted for in this regulation.[10] Department officials stated, and our work confirmed, that since clear cyberspace operations definitions for budgeting purposes do not exist, there can be significant variations in the elements each organization includes in its budget estimate. Additionally, military service officials said they are challenged in providing budget estimates for cyberspace operations as they are still defining what operations and programs are considered cyberspace operations within their respective services. Military service officials in particular noted that, once DOD provides better guidance and definitions, it will be easier for them to provide service-specific budget information. As of May 2011, definitions related to DOD's full-spectrum cyberspace operations remain unclear, including those needed for budgeting purposes.

Concerning the second issue, DOD has operationally merged defensive and offensive cyberspace operations with the creation of U.S. Cyber Command in October 2010, but the department still does not have a designated focal point or methodology for collecting and compiling budget information on full-spectrum cyberspace operations across the department. U.S. Cyber Command has recognized that the department must incorporate integrated defensive and offensive cyberspace operations into all planning efforts.

DOD's organization for cyberspace operations is decentralized and spread across various offices, commands, agencies, and the military services. This decentralization presents challenges with regard to collecting and compiling a complete DOD cyber budget estimate, as various departments and organizations within DOD each include different elements as a part of their cyberspace operations budgets. For example, the Assistant Secretary of Defense for Networks and Information Integration and

[9] DOD Financial Management Regulation 7000.14R, Vol 2B, Chapter 18 *Information Technology* (July 2010).

[10] Office of Management and Budget, Circular No. A-11, which contains guidance on preparing a federal budget, also defines terms and activities involving information technology and other related areas. Executive Office of the President, Office of Management and Budget Circular No. A-11, *Preparation, Submission, and Execution of the Budget* section 53 (July 2010). However, the DOD Financial Management Regulation notes that regardless of the guidance in section 53 of OMB Circular A-11, DOD categorizes information assurance as a major reportable category of the global information grid/information technology/defense information infrastructure.

Chief Information Officer manages the Defense-wide Information Assurance Program, a well-developed and structured program that has existed since 1998 and produces standard budget data for the information assurance portion of cyberspace operations. However, this office does not have responsibility for preparing a departmentwide full-spectrum cyberspace operations budget estimate that includes offensive operations such as computer network attack and exploitation because such activities are associated with multiple program elements that have both cyber and noncyber components.

Three of the four military services found it difficult to generate complete budget estimates for full-spectrum cyberspace operations that included computer network attack and exploitation in response to our standardized requests for such information.[11] Only the Army was able to provide a budget estimate that it believed addressed full-spectrum cyberspace operations. The Air Force, Navy, and Marine Corps provided budget estimates for information assurance and cyber-related programs. Service officials explained that, historically, computer network attack and exploitation have been a part of classified efforts involving signals intelligence, information operations, and cryptography and appropriately have not been identified in the publicly available President's budget. These programs are generally funded through the classified military intelligence and national intelligence program budgets. However, without including this information in its cyberspace operations budget estimates, DOD's and the Congress' view of the financial resources dedicated to these operations are not comprehensive. We present the budget estimates for fiscal years 2012 to 2016 provided by the Army, Air Force, Navy, and Marine Corps on slides 14 to 17 of the enclosed briefing.

For additional information on the results of our work, see slides 3 through 17 of the enclosure.

## Conclusions

DOD has taken many important steps to better organize its cyberspace efforts within a fairly short period of time. Without a complete budget estimate for full-spectrum cyberspace operations though, DOD does not have a complete picture of the resources it is investing in its cyberspace operations. We recognize that this can occur in newly emerging mission areas. However, until DOD can provide a complete budget estimate for these operations, it will be difficult for the department and Congress to obtain an accurate and comprehensive view of the resources devoted to this emerging warfighting domain and make investment trade-off decisions. In light of the need to confront this serious national security challenge and the fiscal constraints the nation is facing, it is important that DOD have better visibility of its cyberspace resources so that the department and Congress may

[11] We asked the military services to provide budget estimates for full-spectrum cyberspace operations to include computer network defense, computer network attack, and computer network exploitation.

prioritize among the program investments needed to defend DOD's computer networks.

## Recommendations for Executive Action

To improve DOD's ability to develop and provide consistent and complete budget estimates for cyberspace operations across the department, we recommend that the Secretary of Defense take the following actions:

- Direct the Under Secretary of Defense for Policy, in coordination with the Chairman of the Joint Chiefs of Staff, U.S. Cyber Command, and other organizations as appropriate, to develop and document cyberspace-related definitions, including identifying specific activities and program elements, for purposes of budgeting for full-spectrum cyberspace operations, that will be used and accepted departmentwide. They should also establish a time frame for completing these actions.

- Designate a single focal point to develop a methodology and provide a single, departmentwide budget estimate and detailed spending data for full-spectrum cyberspace operations (to include computer network defense, attack, and exploitation), including unclassified funding as well as classified data from the military intelligence and national intelligence programs and any other programs, as appropriate.

## Agency Comments and Our Evaluation

In written comments on a draft of this report, DOD partially concurred with our recommendations. DOD agreed with the objective of our recommendation that the Under Secretary of Defense for Policy, in coordination with the Chairman of the Joint Chiefs of Staff and U.S. Cyber Command, should develop and document cyberspace-related definitions for purposes of budgeting for full-spectrum cyberspace operations and establish a time frame for doing so, but did not provide a timeline for completing these actions. DOD noted in its comments that additional components should be included in identifying the specific activities and program elements for purposes of budgeting for full-spectrum cyberspace operations and that to ensure the right organizations are involved, the department should be given discretion to direct implementation of the recommendation. We have adjusted our recommendation to allow the department to include other appropriate organizations at its discretion. We believe that this adjustment will allow the department the flexibility needed to take the actions we recommended and encourage DOD to set a time frame for completing these actions.

DOD also partially concurred with our recommendation to designate a single focal point to develop a methodology and provide a single, departmentwide budget estimate and detailed spending data for full-spectrum cyberspace operations (to include computer network defense, attack, and exploitation), including unclassified funding as well as classified data from the military intelligence and national intelligence programs and any other programs, as appropriate. However, DOD stated that the Office of the Director of National Intelligence must be intimately involved in the development of budget estimates and spending data for classified data related to cyberspace operations that are contained in the national intelligence program and suggested that we include that Office in our recommendation. We agree that the Director of National Intelligence has an important role in cyberspace operations and should be involved in the development of budget estimates and spending data contained in the national intelligence program. We further believe that the Secretary of Defense has the ability to coordinate with the Director of National Intelligence, as appropriate, to take actions necessary to satisfy our recommendation.

DOD's comments are reprinted in their entirety in enclosure II.

- - - - -

We are sending this report to the appropriate congressional committees. We are also sending copies to the Secretary of Defense, the Secretary of the Army, the Secretary of the Navy, the Secretary of the Air Force; the Commandant of the Marine Corps; the Commander of U.S. Strategic Command; and the Commander of U.S. Cyber Command. This report will also be available at no charge on our Web site at http://www.gao.gov.

Should you or your staff have questions concerning this report, please contact Davi M. D'Agostino at (202) 512-5431 or dagostinod@gao.gov; or Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov. Key contributors to this report were Penney Harwell Caramia, Assistant Director; Jeffrey Knott, Assistant Director; Nelsie Alcoser; Katherine Lenane; Jamilah Moon; Zsaroq Powe; and Cheryl Weissman.

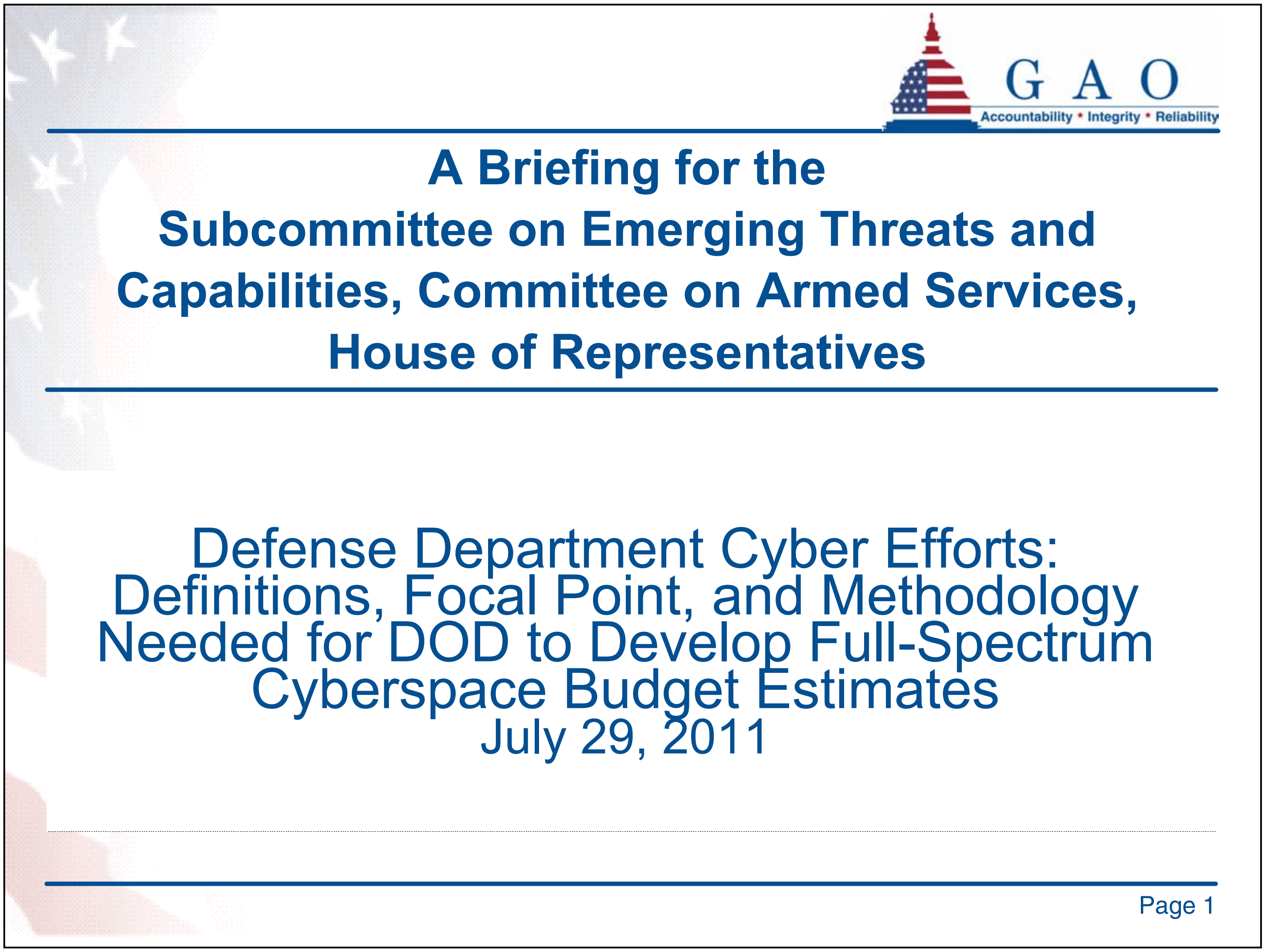
Davi M. D'Agostino

Davi M. D'Agostino
Director
Defense Capabilities and Management

Gregory C. Wilshusen

Gregory C. Wilshusen
Director
Information Technology

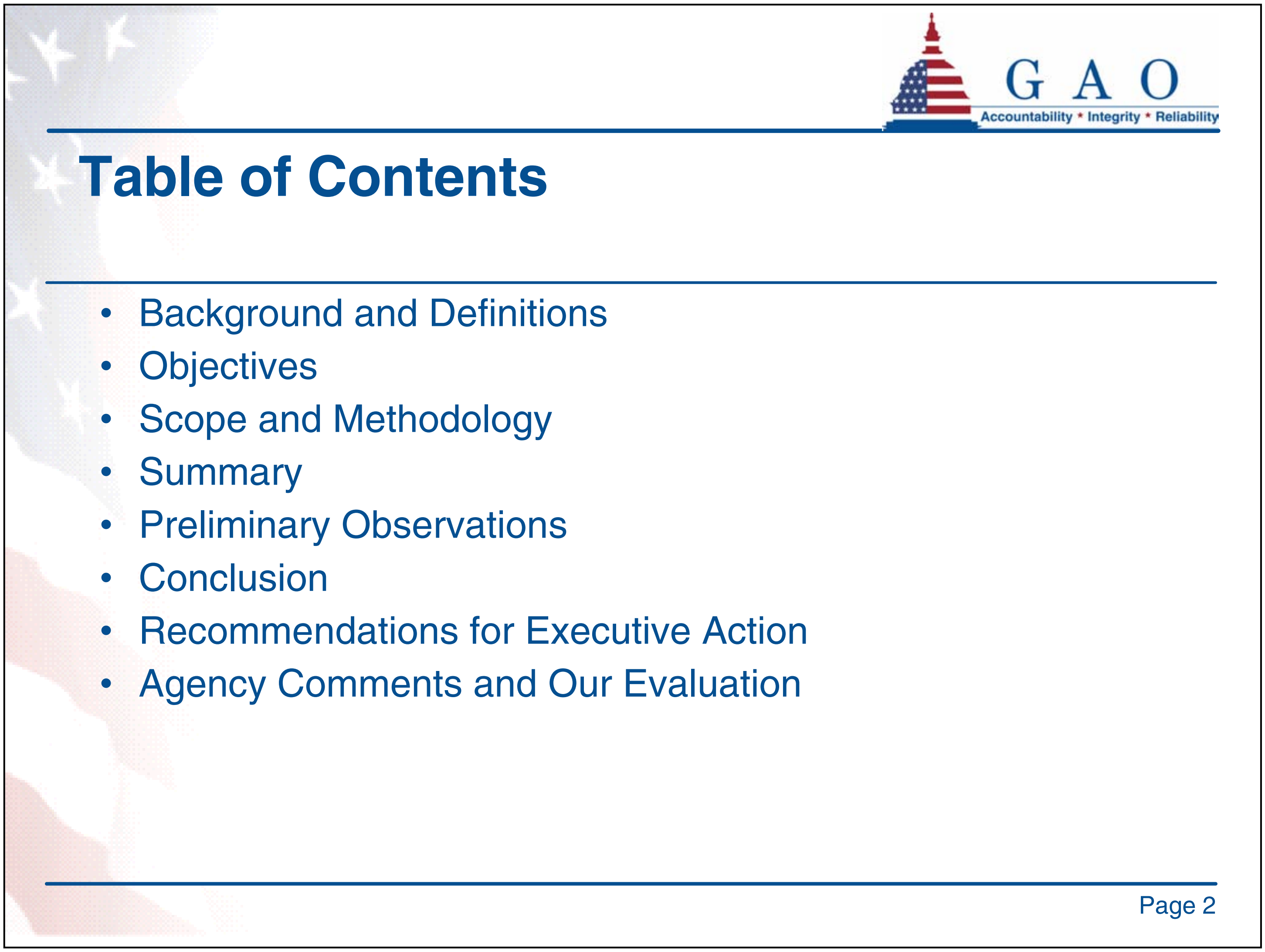
Enclosures



# A Briefing for the Subcommittee on Emerging Threats and Capabilities, Committee on Armed Services, House of Representatives

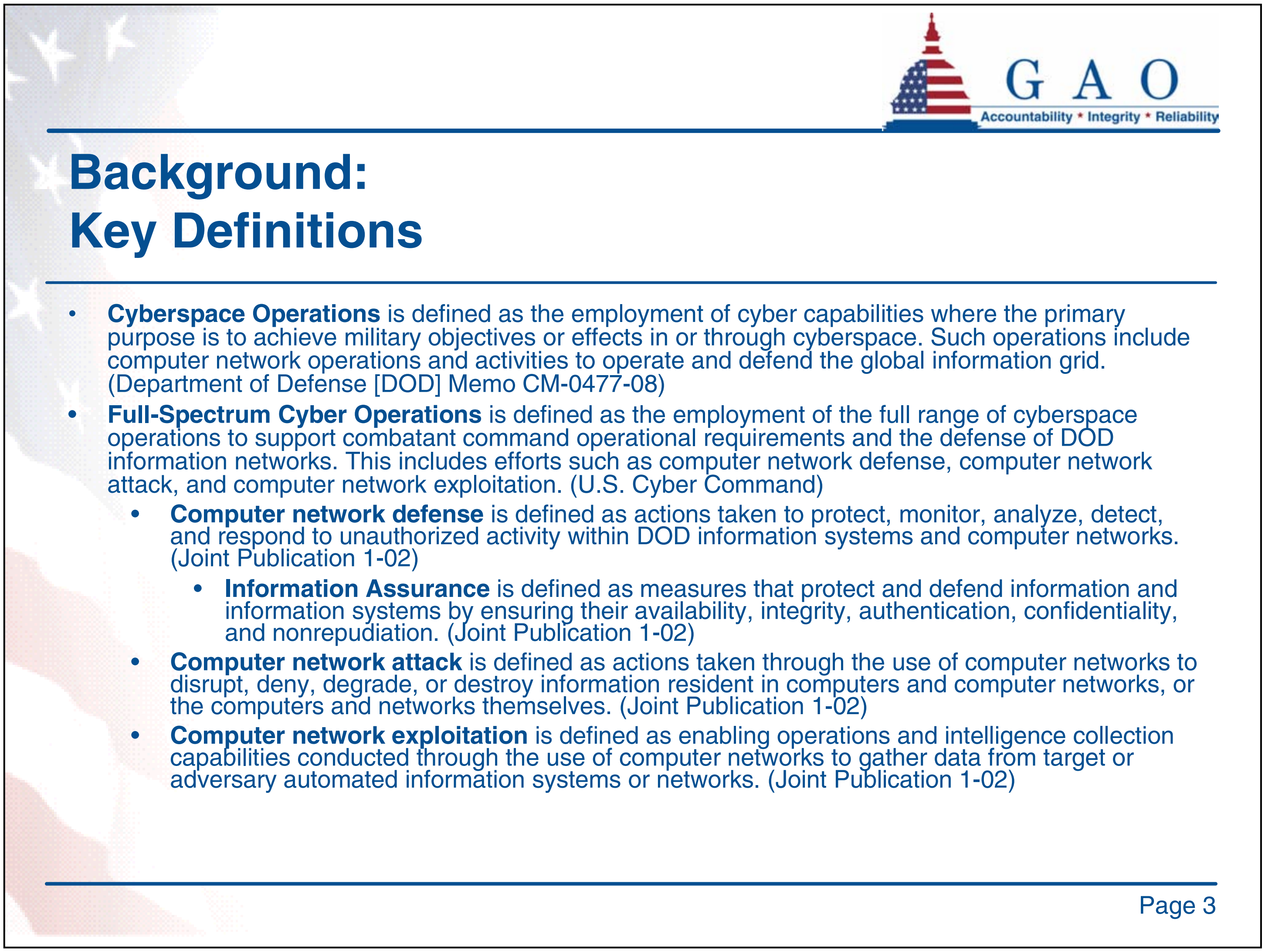
## Defense Department Cyber Efforts: Definitions, Focal Point, and Methodology Needed for DOD to Develop Full-Spectrum Cyberspace Budget Estimates

July 29, 2011



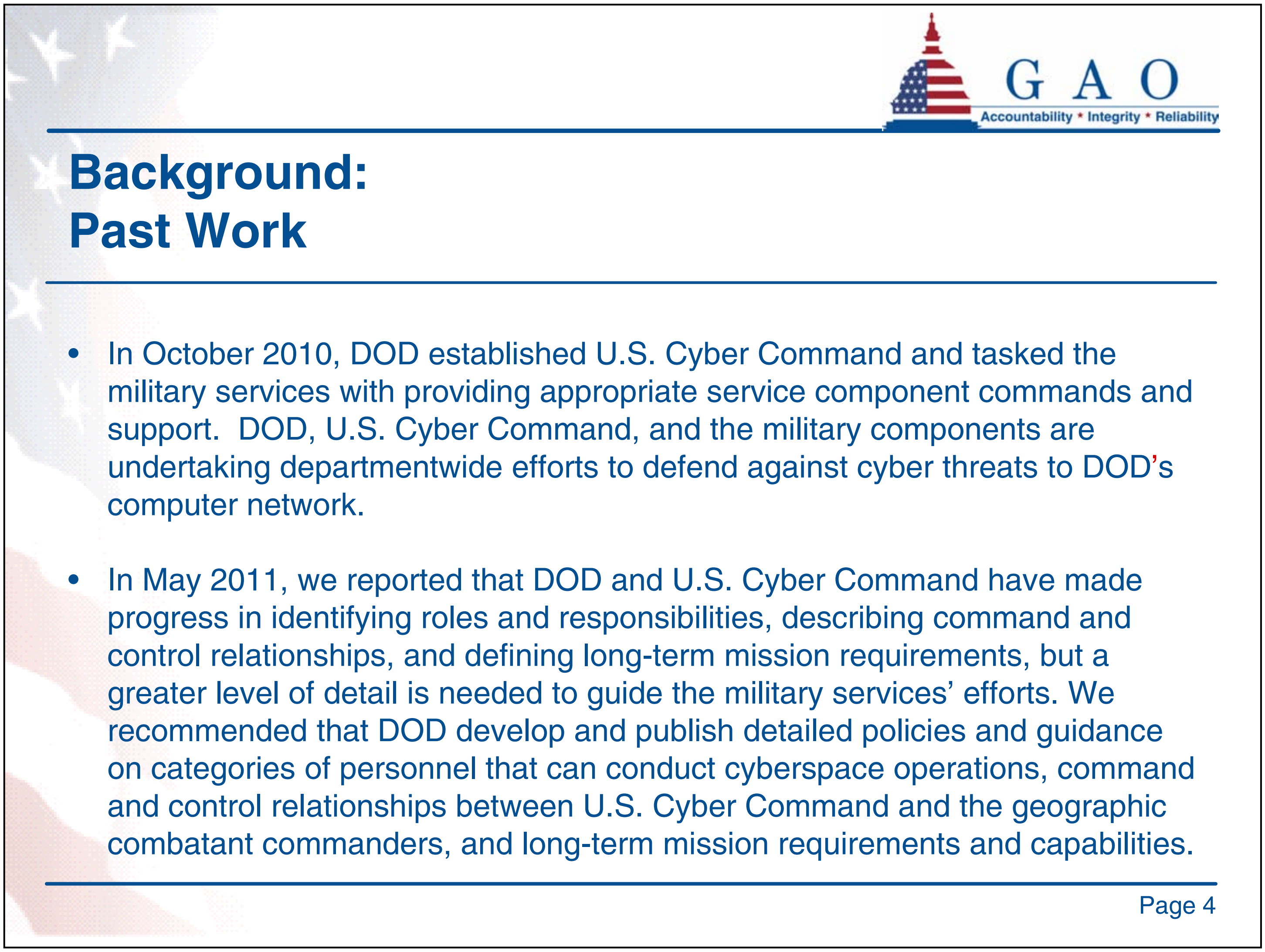
# Table of Contents

- Background and Definitions
- Objectives
- Scope and Methodology
- Summary
- Preliminary Observations
- Conclusion
- Recommendations for Executive Action
- Agency Comments and Our Evaluation



# Background:
# Key Definitions

- **Cyberspace Operations** is defined as the employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace. Such operations include computer network operations and activities to operate and defend the global information grid. (Department of Defense [DOD] Memo CM-0477-08)
- **Full-Spectrum Cyber Operations** is defined as the employment of the full range of cyberspace operations to support combatant command operational requirements and the defense of DOD information networks. This includes efforts such as computer network defense, computer network attack, and computer network exploitation. (U.S. Cyber Command)
  - **Computer network defense** is defined as actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within DOD information systems and computer networks. (Joint Publication 1-02)
    - **Information Assurance** is defined as measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. (Joint Publication 1-02)
  - **Computer network attack** is defined as actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. (Joint Publication 1-02)
  - **Computer network exploitation** is defined as enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks. (Joint Publication 1-02)

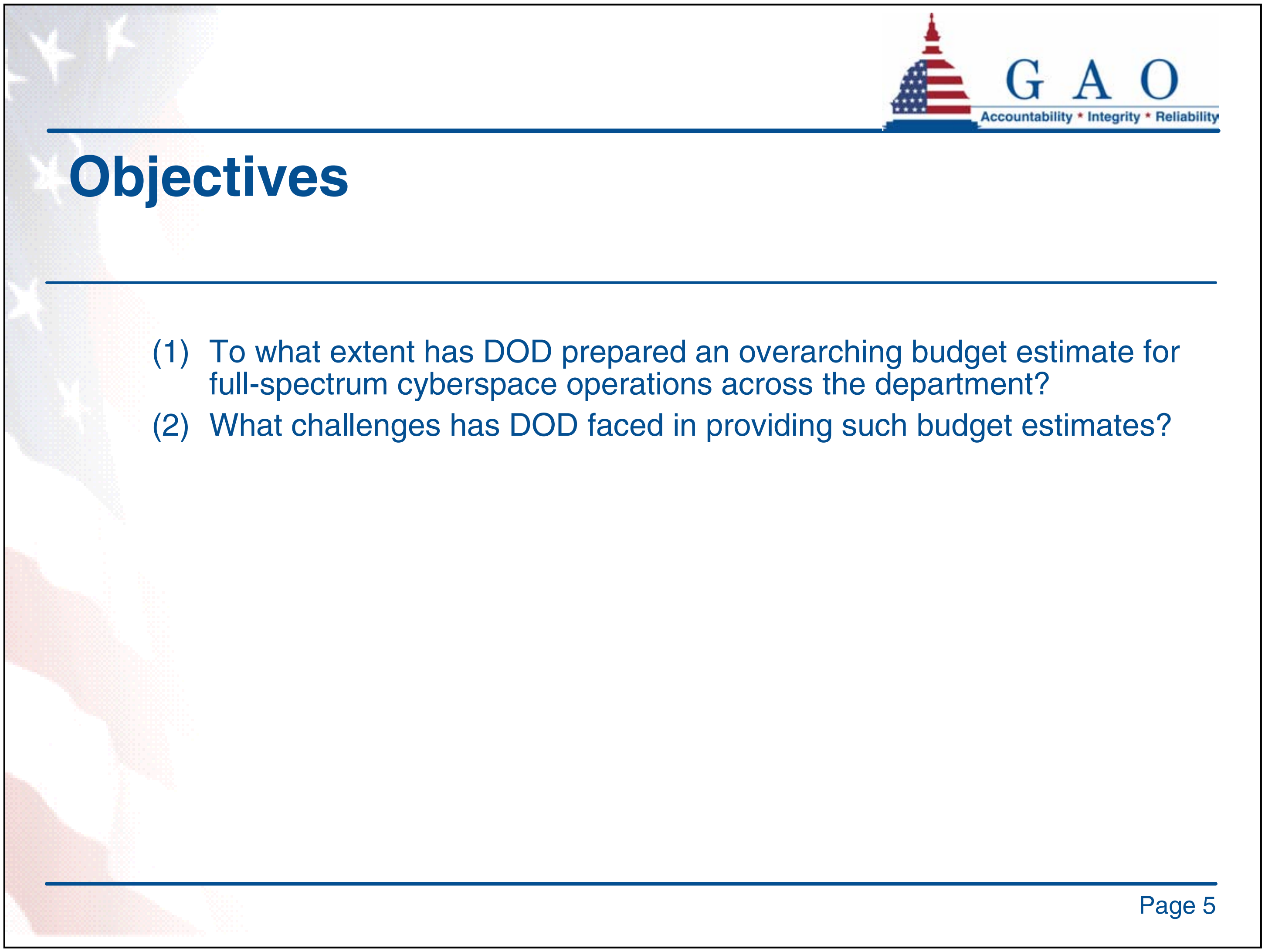


GAO
Accountability * Integrity * Reliability

## Background: Past Work

- In October 2010, DOD established U.S. Cyber Command and tasked the military services with providing appropriate service component commands and support. DOD, U.S. Cyber Command, and the military components are undertaking departmentwide efforts to defend against cyber threats to DOD's computer network.

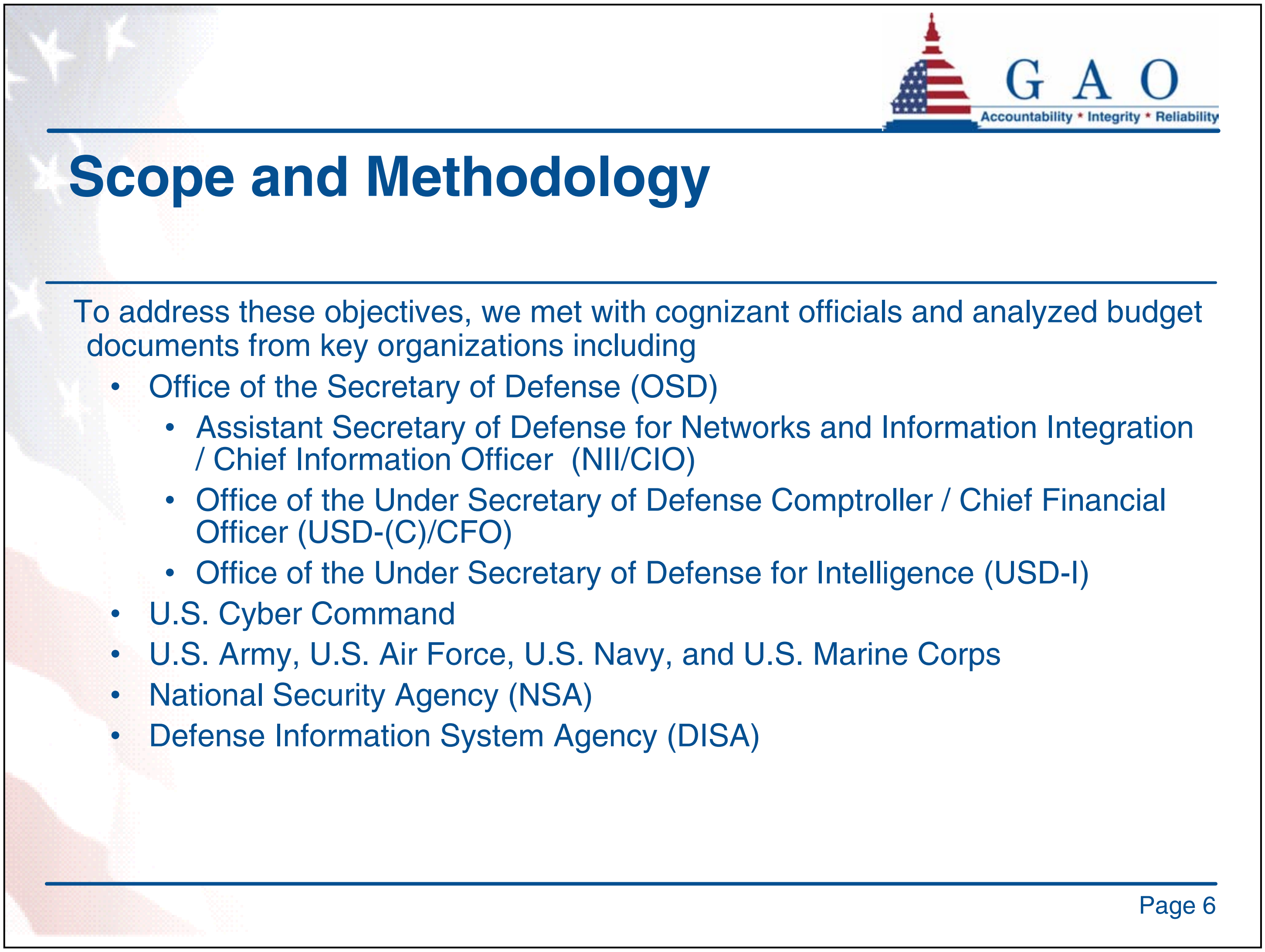
- In May 2011, we reported that DOD and U.S. Cyber Command have made progress in identifying roles and responsibilities, describing command and control relationships, and defining long-term mission requirements, but a greater level of detail is needed to guide the military services' efforts. We recommended that DOD develop and publish detailed policies and guidance on categories of personnel that can conduct cyberspace operations, command and control relationships between U.S. Cyber Command and the geographic combatant commanders, and long-term mission requirements and capabilities.



# Objectives

(1) To what extent has DOD prepared an overarching budget estimate for full-spectrum cyberspace operations across the department?

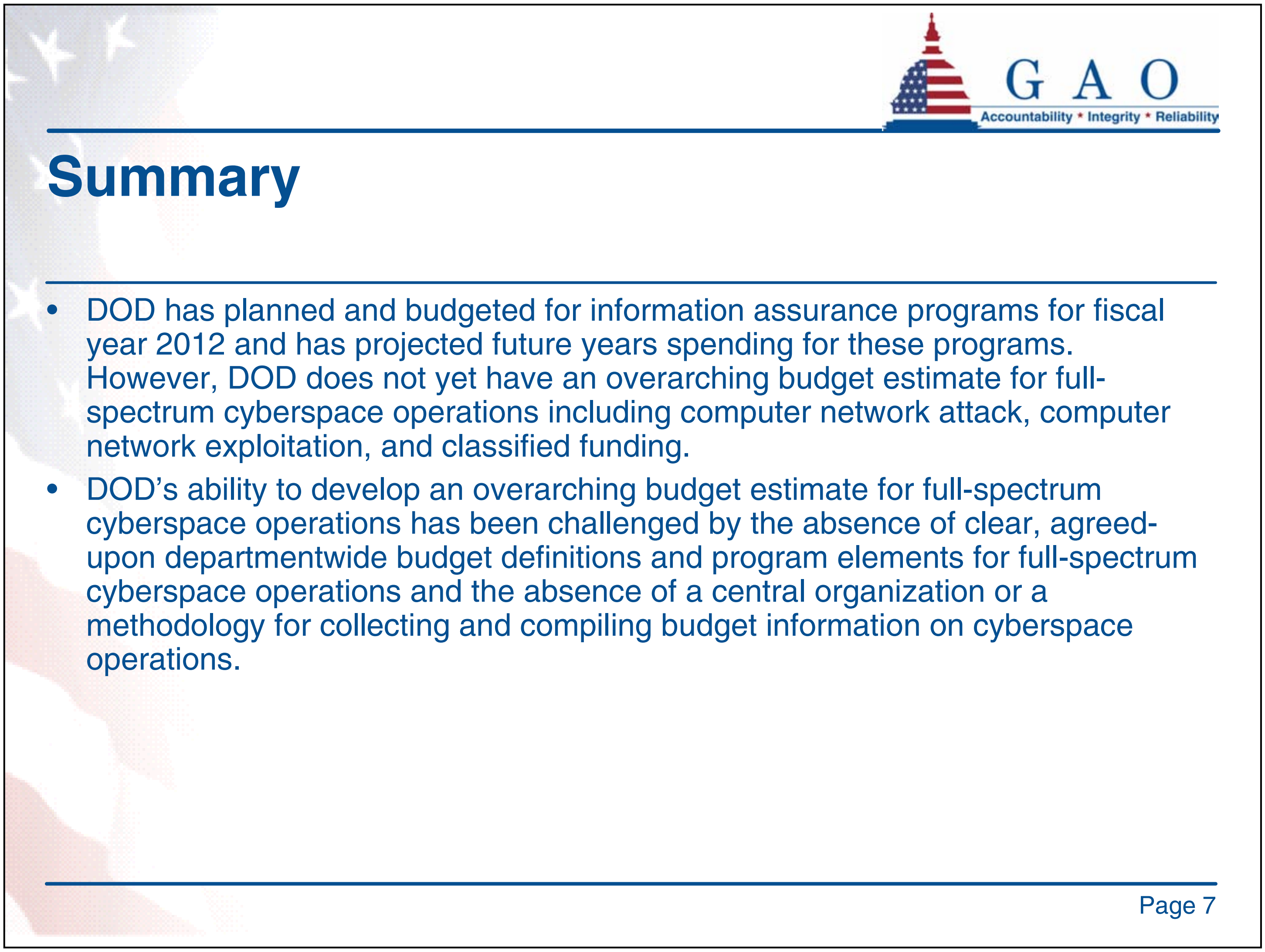
(2) What challenges has DOD faced in providing such budget estimates?



# Scope and Methodology

To address these objectives, we met with cognizant officials and analyzed budget documents from key organizations including

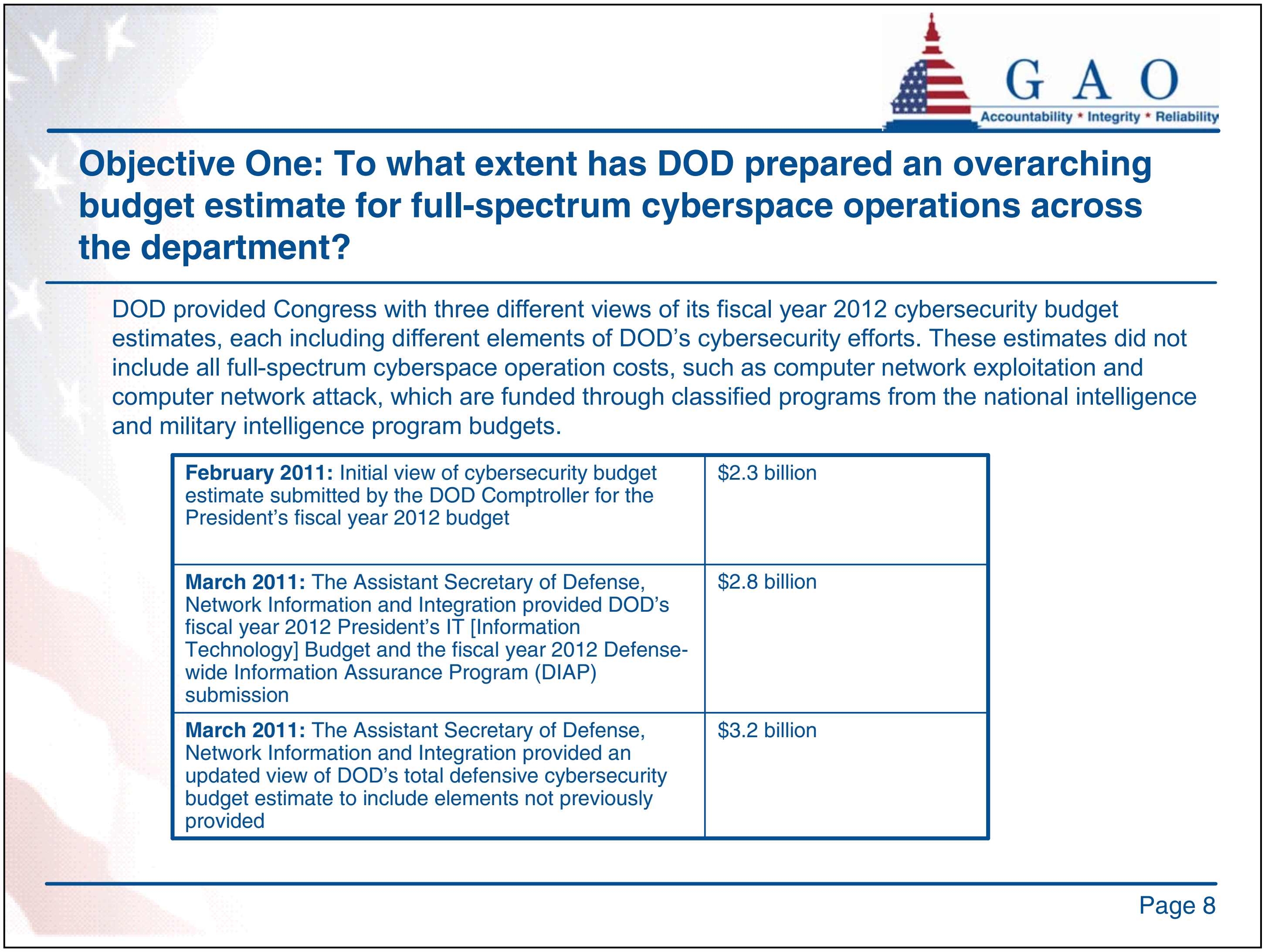
- Office of the Secretary of Defense (OSD)
  - Assistant Secretary of Defense for Networks and Information Integration / Chief Information Officer  (NII/CIO)
  - Office of the Under Secretary of Defense Comptroller / Chief Financial Officer (USD-(C)/CFO)
  - Office of the Under Secretary of Defense for Intelligence (USD-I)
- U.S. Cyber Command
- U.S. Army, U.S. Air Force, U.S. Navy, and U.S. Marine Corps
- National Security Agency (NSA)
- Defense Information System Agency (DISA)



## Summary

- DOD has planned and budgeted for information assurance programs for fiscal year 2012 and has projected future years spending for these programs. However, DOD does not yet have an overarching budget estimate for full-spectrum cyberspace operations including computer network attack, computer network exploitation, and classified funding.
- DOD's ability to develop an overarching budget estimate for full-spectrum cyberspace operations has been challenged by the absence of clear, agreed-upon departmentwide budget definitions and program elements for full-spectrum cyberspace operations and the absence of a central organization or a methodology for collecting and compiling budget information on cyberspace operations.

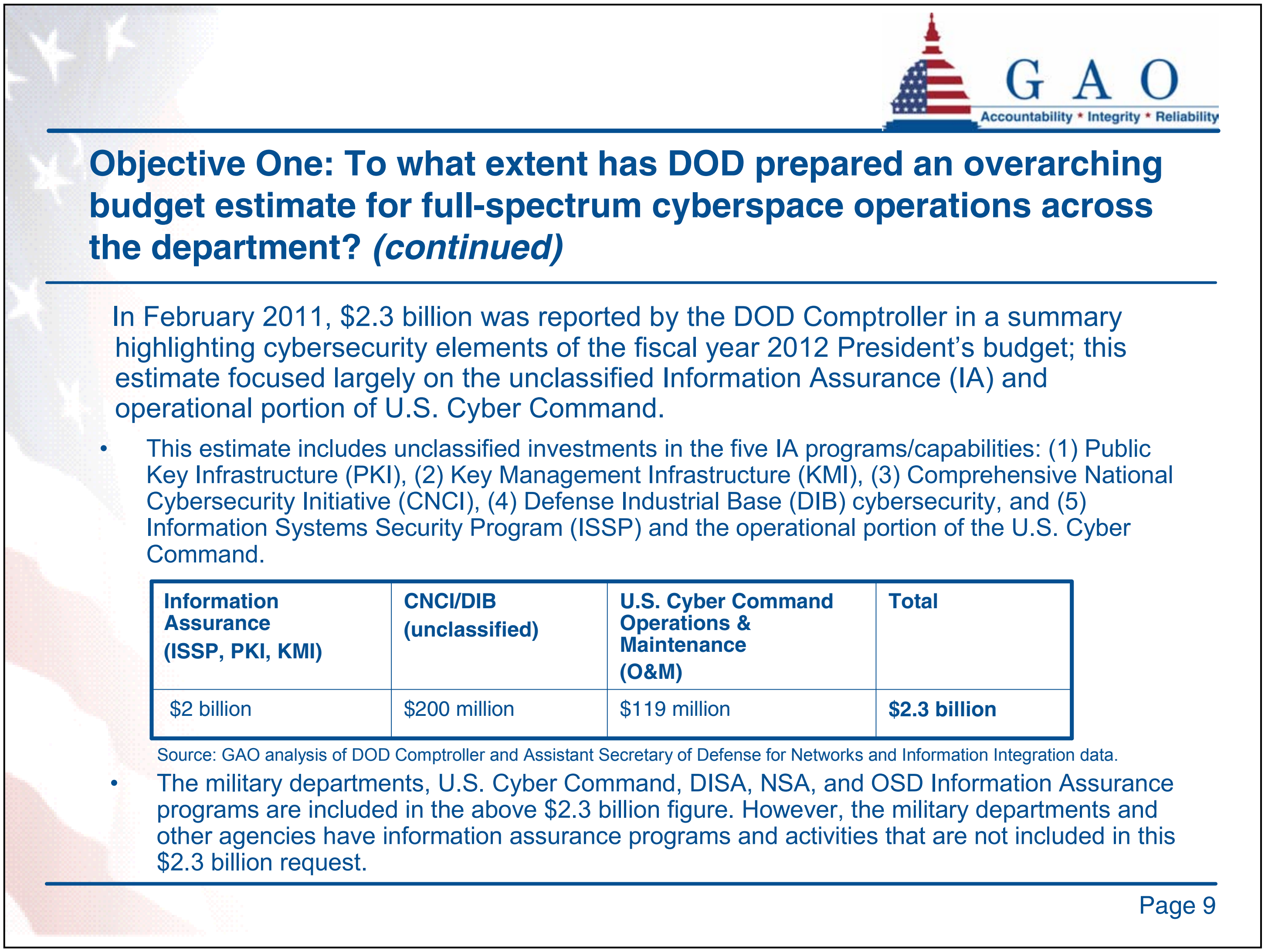
Page 7



## Objective One: To what extent has DOD prepared an overarching budget estimate for full-spectrum cyberspace operations across the department?

DOD provided Congress with three different views of its fiscal year 2012 cybersecurity budget estimates, each including different elements of DOD's cybersecurity efforts. These estimates did not include all full-spectrum cyberspace operation costs, such as computer network exploitation and computer network attack, which are funded through classified programs from the national intelligence and military intelligence program budgets.

| | |
|---|---|
| **February 2011:** Initial view of cybersecurity budget estimate submitted by the DOD Comptroller for the President's fiscal year 2012 budget | $2.3 billion |
| **March 2011:** The Assistant Secretary of Defense, Network Information and Integration provided DOD's fiscal year 2012 President's IT [Information Technology] Budget and the fiscal year 2012 Defense-wide Information Assurance Program (DIAP) submission | $2.8 billion |
| **March 2011:** The Assistant Secretary of Defense, Network Information and Integration provided an updated view of DOD's total defensive cybersecurity budget estimate to include elements not previously provided | $3.2 billion |



## Objective One: To what extent has DOD prepared an overarching budget estimate for full-spectrum cyberspace operations across the department? *(continued)*

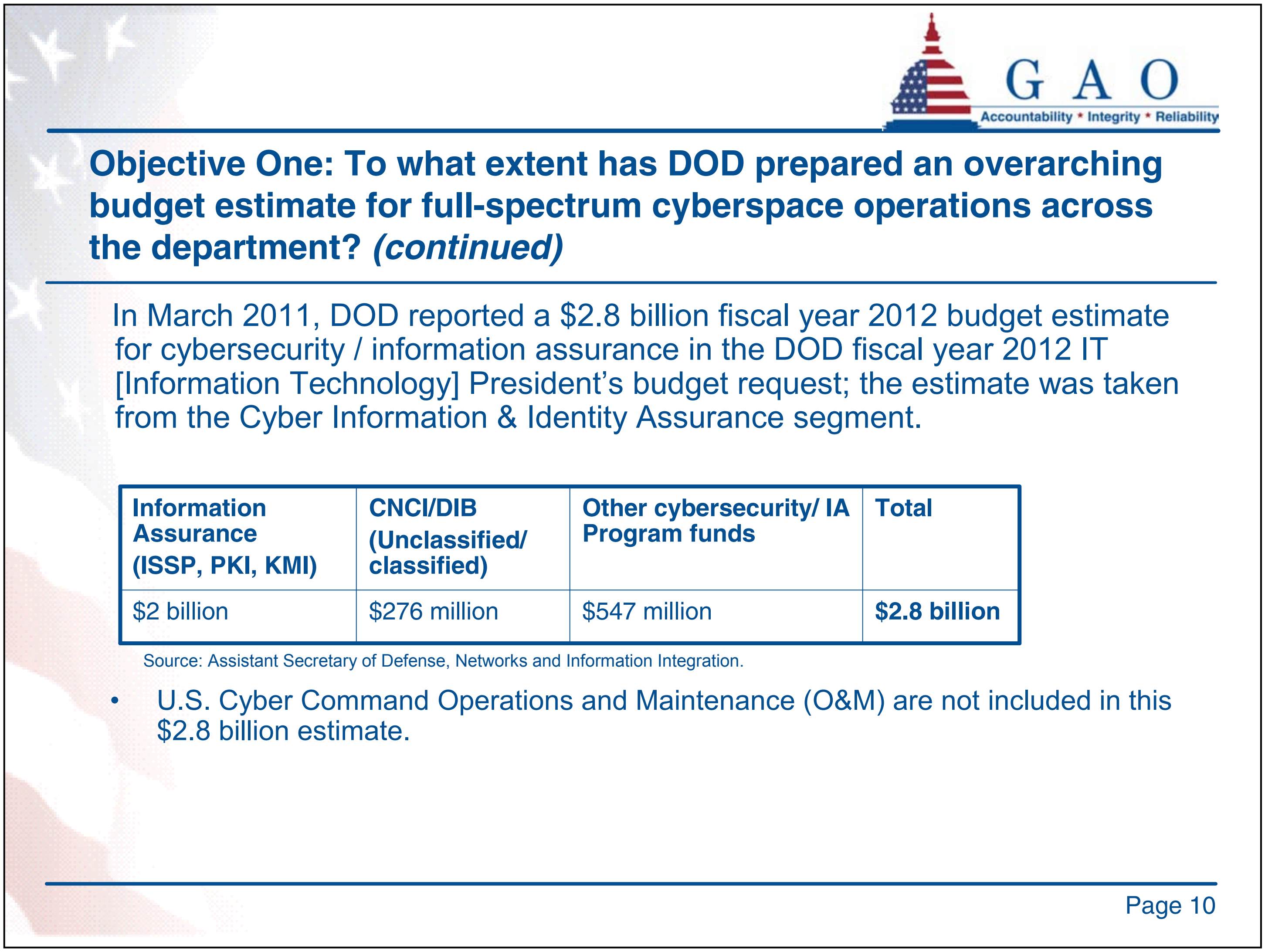
In February 2011, $2.3 billion was reported by the DOD Comptroller in a summary highlighting cybersecurity elements of the fiscal year 2012 President's budget; this estimate focused largely on the unclassified Information Assurance (IA) and operational portion of U.S. Cyber Command.

- This estimate includes unclassified investments in the five IA programs/capabilities: (1) Public Key Infrastructure (PKI), (2) Key Management Infrastructure (KMI), (3) Comprehensive National Cybersecurity Initiative (CNCI), (4) Defense Industrial Base (DIB) cybersecurity, and (5) Information Systems Security Program (ISSP) and the operational portion of the U.S. Cyber Command.

| Information Assurance (ISSP, PKI, KMI) | CNCI/DIB (unclassified) | U.S. Cyber Command Operations & Maintenance (O&M) | Total |
|---|---|---|---|
| $2 billion | $200 million | $119 million | **$2.3 billion** |

Source: GAO analysis of DOD Comptroller and Assistant Secretary of Defense for Networks and Information Integration data.

- The military departments, U.S. Cyber Command, DISA, NSA, and OSD Information Assurance programs are included in the above $2.3 billion figure. However, the military departments and other agencies have information assurance programs and activities that are not included in this $2.3 billion request.



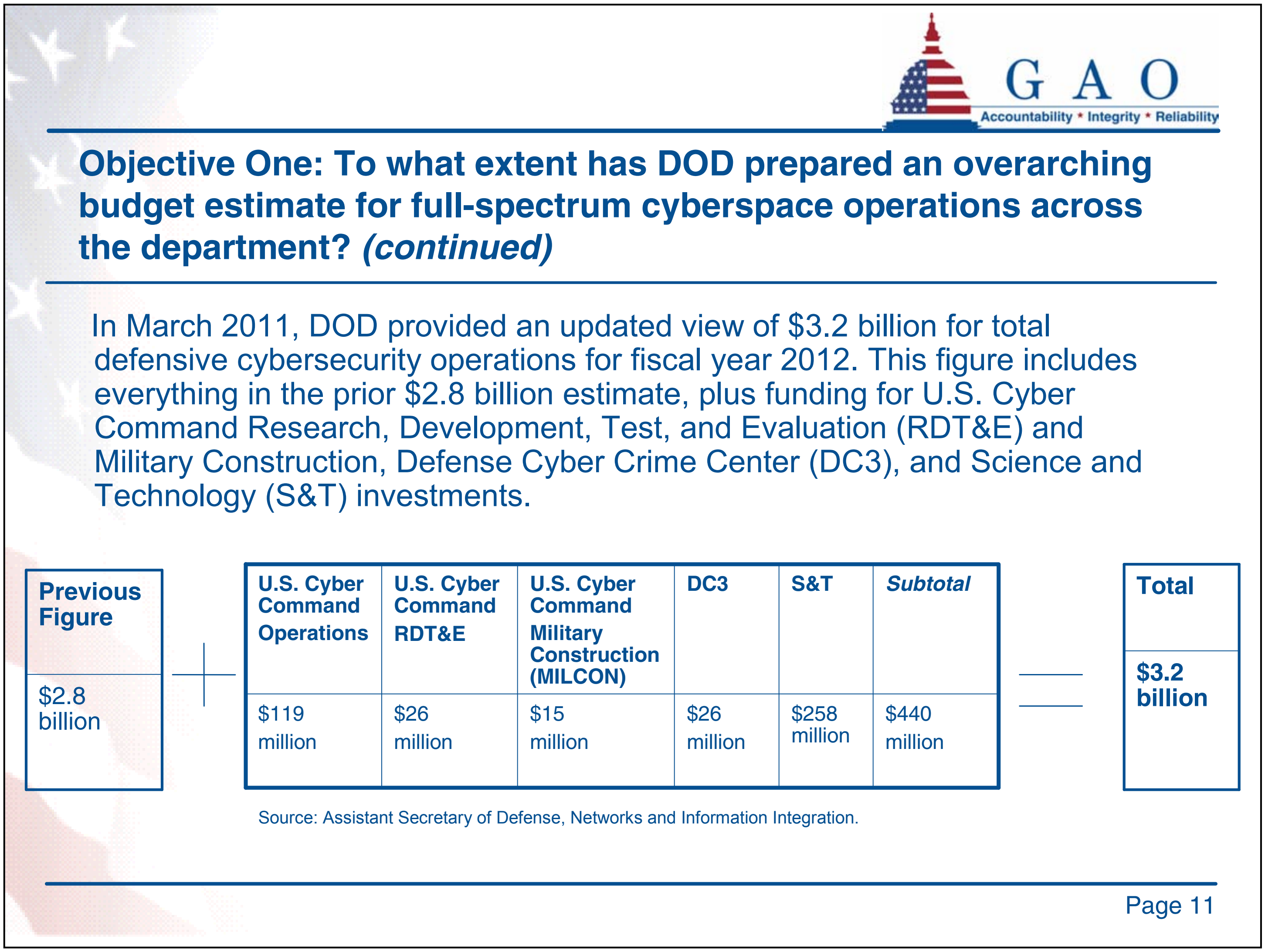
## Objective One: To what extent has DOD prepared an overarching budget estimate for full-spectrum cyberspace operations across the department? *(continued)*

In March 2011, DOD reported a $2.8 billion fiscal year 2012 budget estimate for cybersecurity / information assurance in the DOD fiscal year 2012 IT [Information Technology] President's budget request; the estimate was taken from the Cyber Information & Identity Assurance segment.

| **Information Assurance<br>(ISSP, PKI, KMI)** | **CNCI/DIB<br>(Unclassified/ classified)** | **Other cybersecurity/ IA Program funds** | **Total** |
|---|---|---|---|
| $2 billion | $276 million | $547 million | **$2.8 billion** |

Source: Assistant Secretary of Defense, Networks and Information Integration.

- U.S. Cyber Command Operations and Maintenance (O&M) are not included in this $2.8 billion estimate.

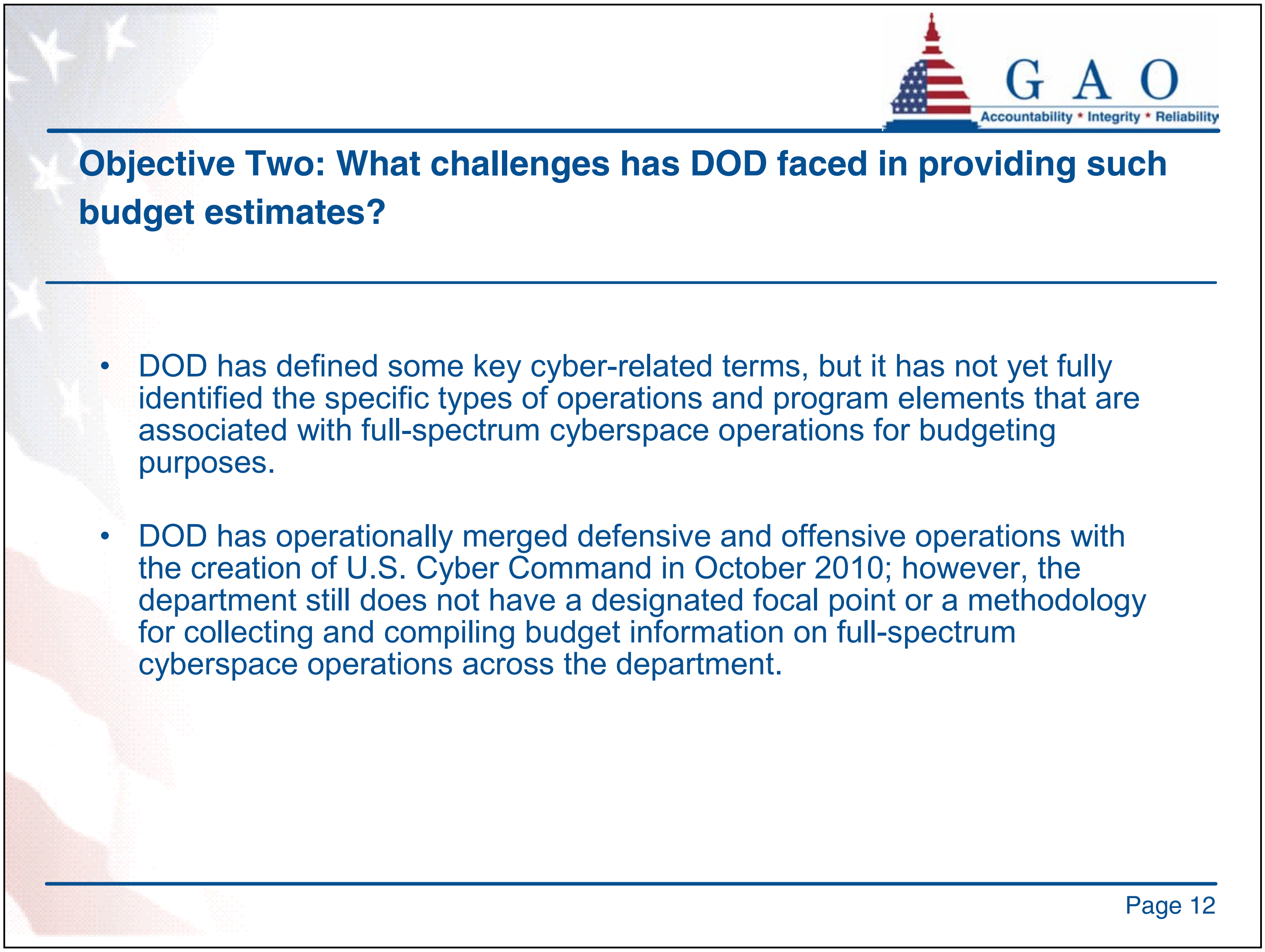


## Objective One: To what extent has DOD prepared an overarching budget estimate for full-spectrum cyberspace operations across the department? *(continued)*

In March 2011, DOD provided an updated view of $3.2 billion for total defensive cybersecurity operations for fiscal year 2012. This figure includes everything in the prior $2.8 billion estimate, plus funding for U.S. Cyber Command Research, Development, Test, and Evaluation (RDT&E) and Military Construction, Defense Cyber Crime Center (DC3), and Science and Technology (S&T) investments.

| **Previous Figure** | | **U.S. Cyber Command Operations** | **U.S. Cyber Command RDT&E** | **U.S. Cyber Command Military Construction (MILCON)** | **DC3** | **S&T** | ***Subtotal*** | | **Total** |
|---|---|---|---|---|---|---|---|---|---|
| $2.8 billion | + | $119 million | $26 million | $15 million | $26 million | $258 million | $440 million | = | **$3.2 billion** |

Source: Assistant Secretary of Defense, Networks and Information Integration.

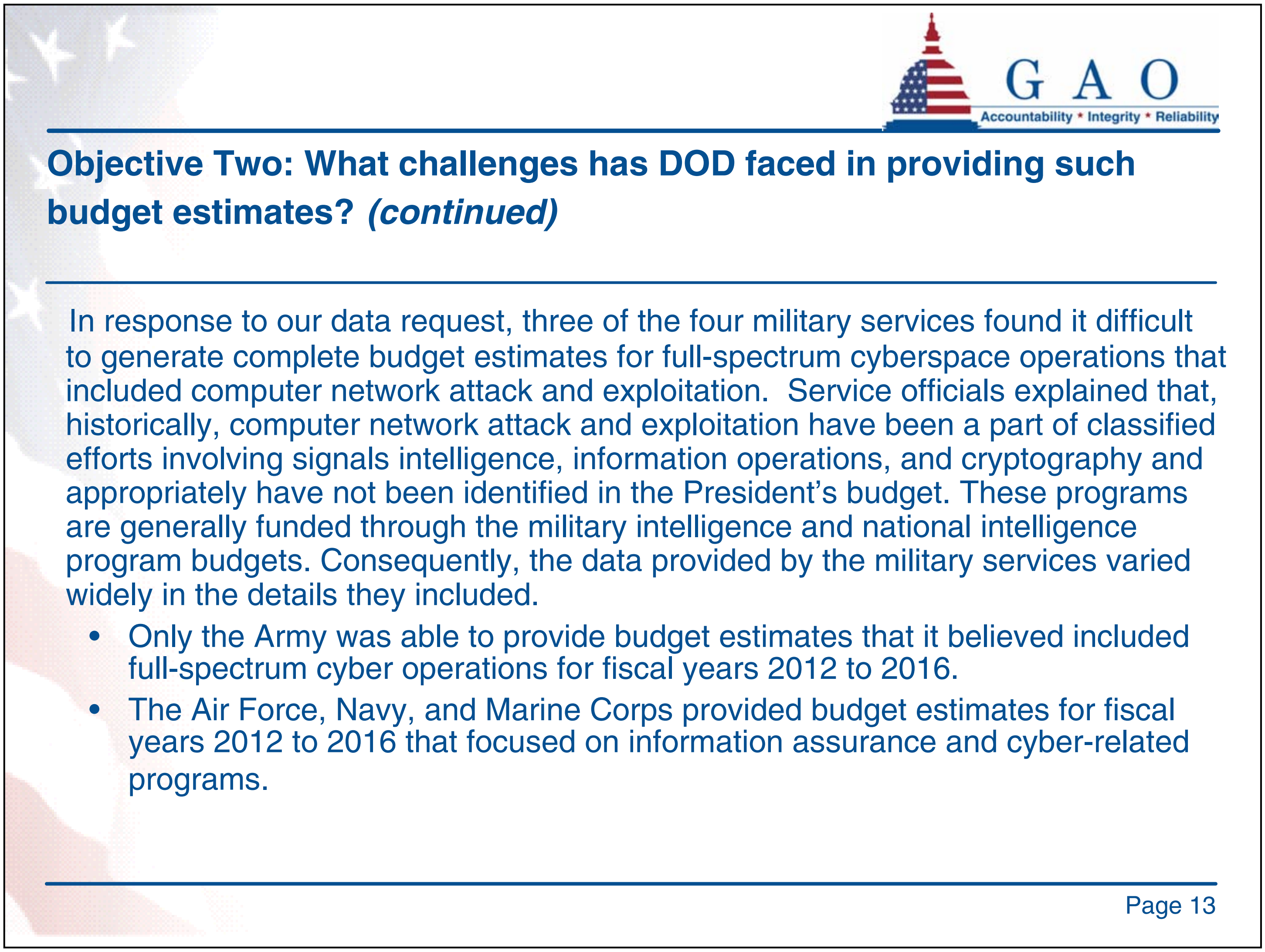


GAO
Accountability * Integrity * Reliability

## Objective Two: What challenges has DOD faced in providing such budget estimates?

- DOD has defined some key cyber-related terms, but it has not yet fully identified the specific types of operations and program elements that are associated with full-spectrum cyberspace operations for budgeting purposes.
- DOD has operationally merged defensive and offensive operations with the creation of U.S. Cyber Command in October 2010; however, the department still does not have a designated focal point or a methodology for collecting and compiling budget information on full-spectrum cyberspace operations across the department.

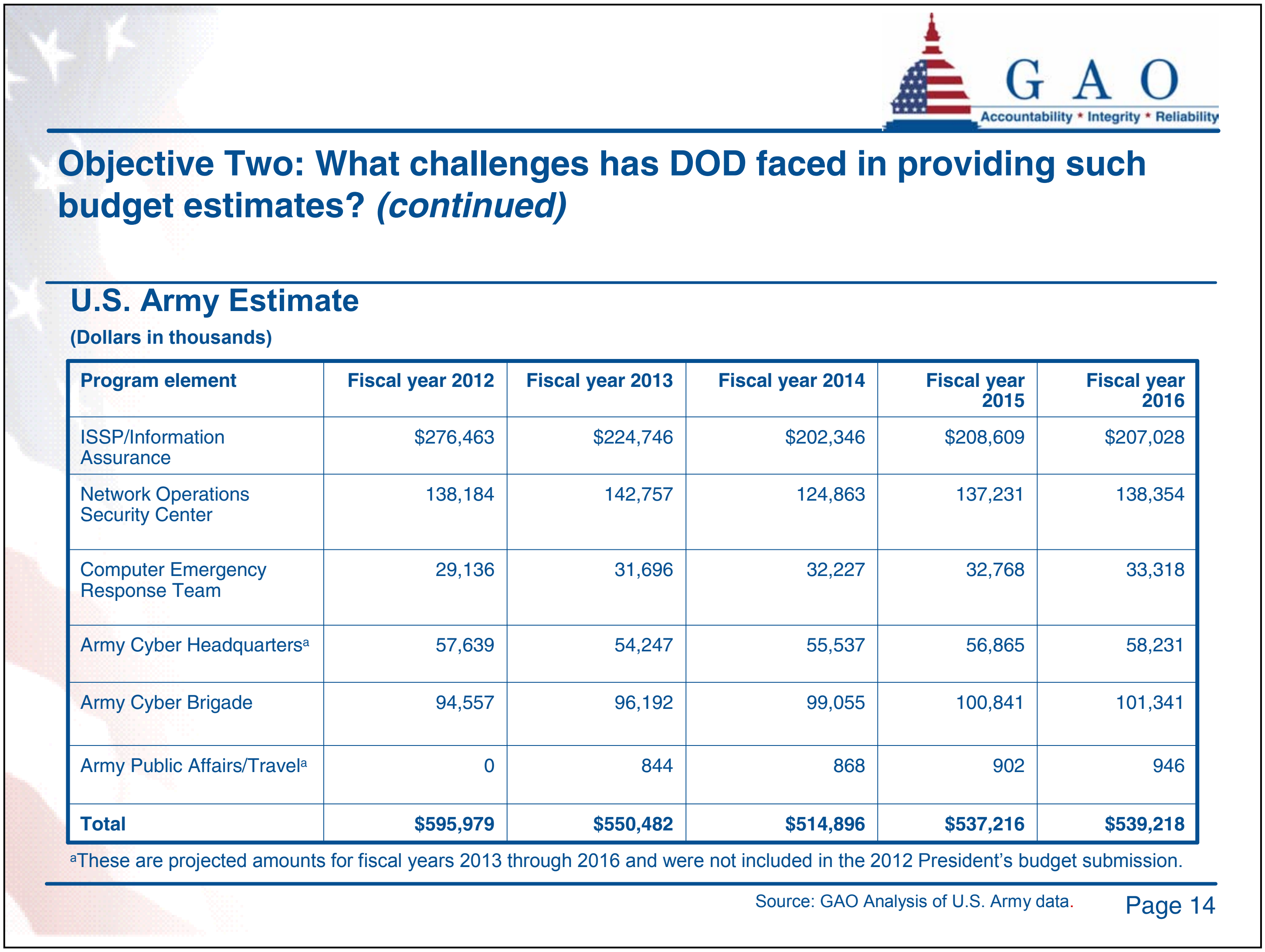
Page 12



## Objective Two: What challenges has DOD faced in providing such budget estimates? *(continued)*

In response to our data request, three of the four military services found it difficult to generate complete budget estimates for full-spectrum cyberspace operations that included computer network attack and exploitation. Service officials explained that, historically, computer network attack and exploitation have been a part of classified efforts involving signals intelligence, information operations, and cryptography and appropriately have not been identified in the President's budget. These programs are generally funded through the military intelligence and national intelligence program budgets. Consequently, the data provided by the military services varied widely in the details they included.

- Only the Army was able to provide budget estimates that it believed included full-spectrum cyber operations for fiscal years 2012 to 2016.
- The Air Force, Navy, and Marine Corps provided budget estimates for fiscal years 2012 to 2016 that focused on information assurance and cyber-related programs.



## Objective Two: What challenges has DOD faced in providing such budget estimates? *(continued)*

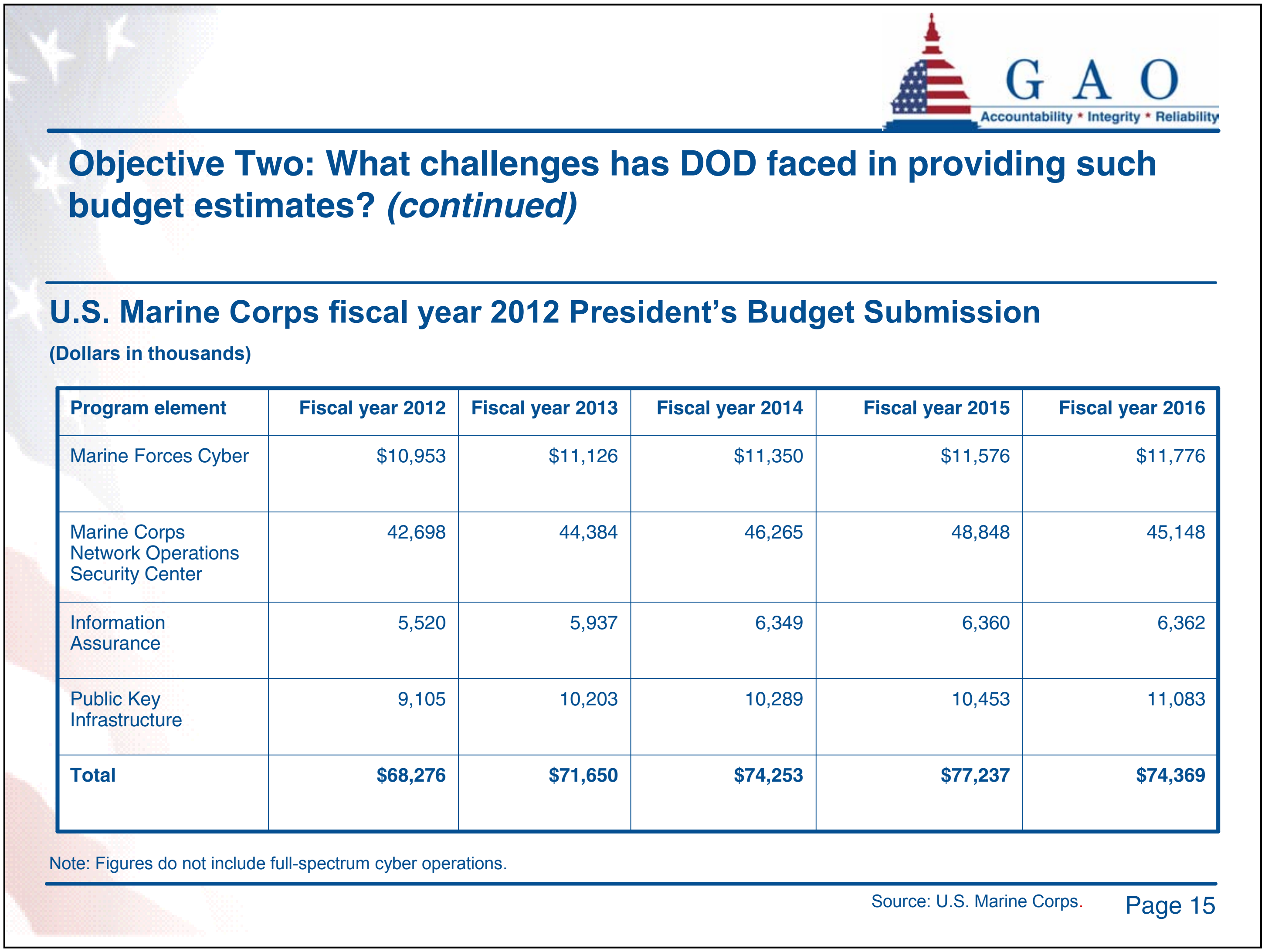
### U.S. Army Estimate

**(Dollars in thousands)**

| Program element | Fiscal year 2012 | Fiscal year 2013 | Fiscal year 2014 | Fiscal year 2015 | Fiscal year 2016 |
|---|---:|---:|---:|---:|---:|
| ISSP/Information Assurance | $276,463 | $224,746 | $202,346 | $208,609 | $207,028 |
| Network Operations Security Center | 138,184 | 142,757 | 124,863 | 137,231 | 138,354 |
| Computer Emergency Response Team | 29,136 | 31,696 | 32,227 | 32,768 | 33,318 |
| Army Cyber Headquarters[a] | 57,639 | 54,247 | 55,537 | 56,865 | 58,231 |
| Army Cyber Brigade | 94,557 | 96,192 | 99,055 | 100,841 | 101,341 |
| Army Public Affairs/Travel[a] | 0 | 844 | 868 | 902 | 946 |
| **Total** | **$595,979** | **$550,482** | **$514,896** | **$537,216** | **$539,218** |

[a] These are projected amounts for fiscal years 2013 through 2016 and were not included in the 2012 President's budget submission.

Source: GAO Analysis of U.S. Army data.



## Objective Two: What challenges has DOD faced in providing such budget estimates? *(continued)*

### U.S. Marine Corps fiscal year 2012 President's Budget Submission

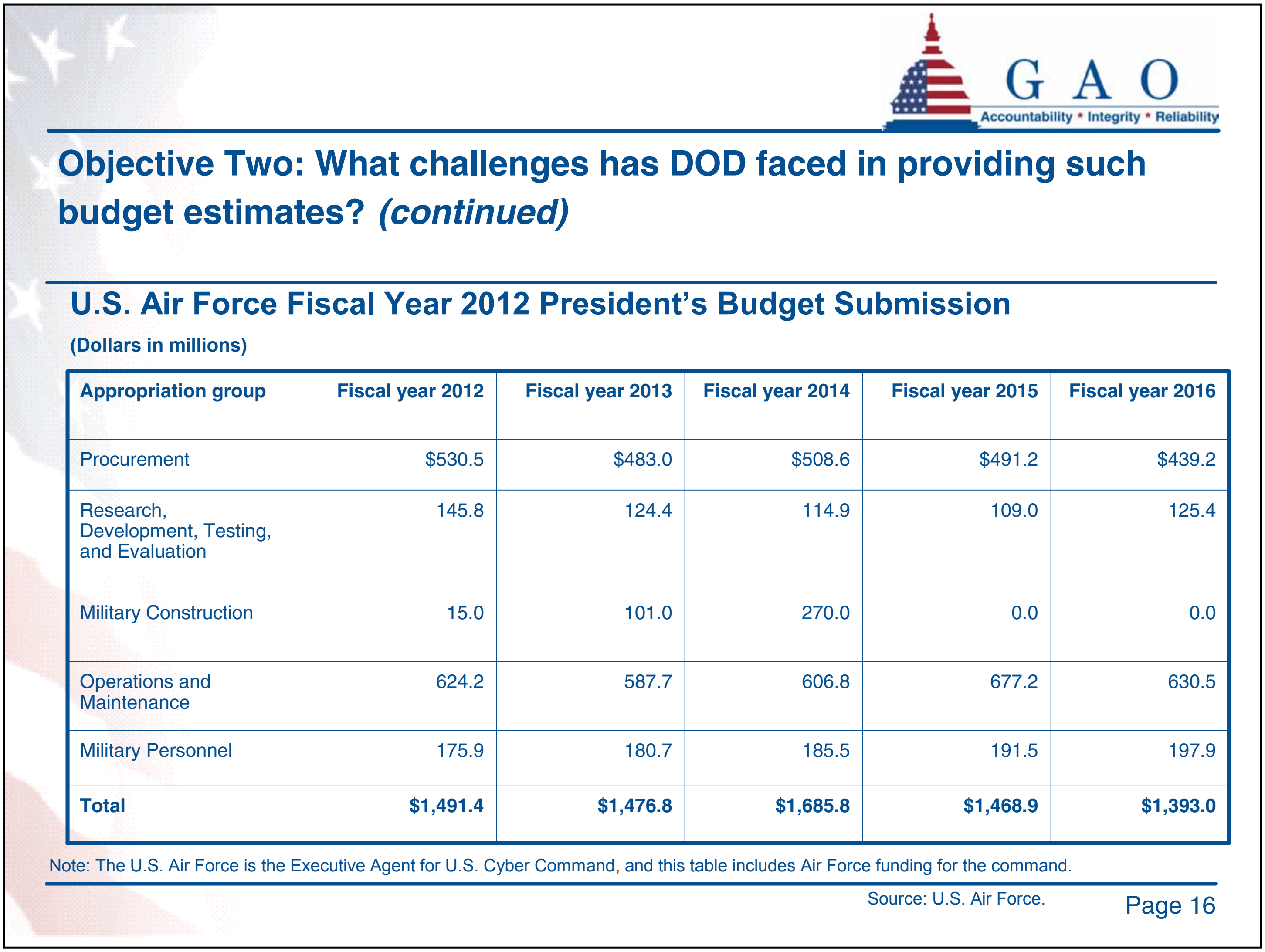
**(Dollars in thousands)**

| Program element | Fiscal year 2012 | Fiscal year 2013 | Fiscal year 2014 | Fiscal year 2015 | Fiscal year 2016 |
|---|---|---|---|---|---|
| Marine Forces Cyber | $10,953 | $11,126 | $11,350 | $11,576 | $11,776 |
| Marine Corps Network Operations Security Center | 42,698 | 44,384 | 46,265 | 48,848 | 45,148 |
| Information Assurance | 5,520 | 5,937 | 6,349 | 6,360 | 6,362 |
| Public Key Infrastructure | 9,105 | 10,203 | 10,289 | 10,453 | 11,083 |
| **Total** | **$68,276** | **$71,650** | **$74,253** | **$77,237** | **$74,369** |

Note: Figures do not include full-spectrum cyber operations.

Source: U.S. Marine Corps.

Page 15



## Objective Two: What challenges has DOD faced in providing such budget estimates? *(continued)*

### U.S. Air Force Fiscal Year 2012 President's Budget Submission

**(Dollars in millions)**

| Appropriation group | Fiscal year 2012 | Fiscal year 2013 | Fiscal year 2014 | Fiscal year 2015 | Fiscal year 2016 |
|---|---|---|---|---|---|
| Procurement | $530.5 | $483.0 | $508.6 | $491.2 | $439.2 |
| Research, Development, Testing, and Evaluation | 145.8 | 124.4 | 114.9 | 109.0 | 125.4 |
| Military Construction | 15.0 | 101.0 | 270.0 | 0.0 | 0.0 |
| Operations and Maintenance | 624.2 | 587.7 | 606.8 | 677.2 | 630.5 |
| Military Personnel | 175.9 | 180.7 | 185.5 | 191.5 | 197.9 |
| **Total** | **$1,491.4** | **$1,476.8** | **$1,685.8** | **$1,468.9** | **$1,393.0** |

Note: The U.S. Air Force is the Executive Agent for U.S. Cyber Command, and this table includes Air Force funding for the command.

Source: U.S. Air Force.

Page 16

## Objective Two: What challenges has DOD faced in providing such budget estimates? *(continued)*

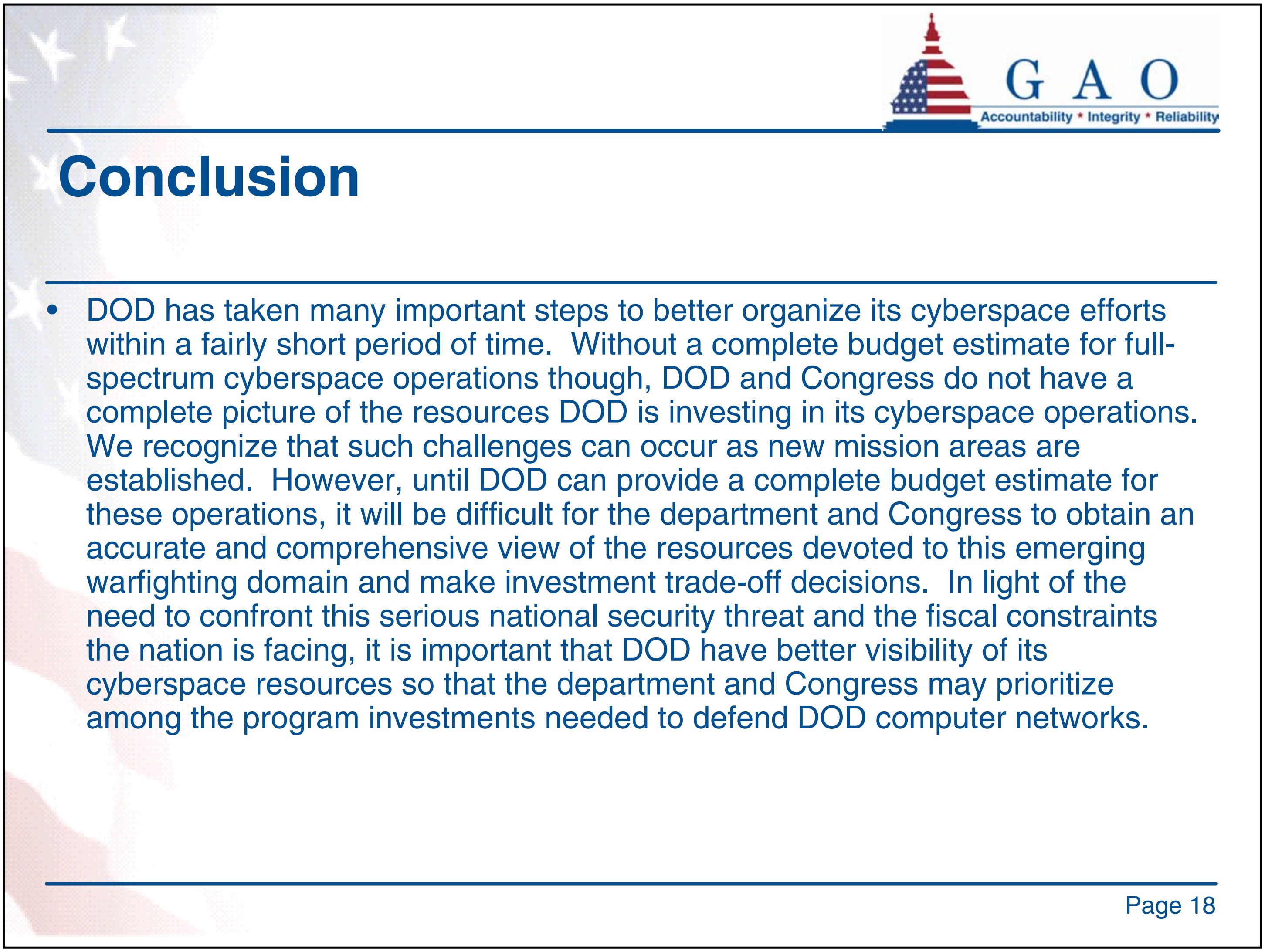
### U.S. Navy Fiscal Year 2012 National Security System President's Budget Information Technology Budget

**(Dollars in thousands)**

| Appropriation group | Fiscal year 2012 | Fiscal year 2013 | Fiscal year 2014 | Fiscal year 2015 | Fiscal year 2016 |
|---|---|---|---|---|---|
| Procurement | $627,134 | $813,619 | $900,513 | $834,644 | $897,445 |
| Research, Development, Testing, and Evaluation | 914,049 | 359,978 | 284,963 | 231,063 | 258,322 |
| Working Capital Fund | 292,378 | 286,740 | 290,350 | 295,225 | 295,193 |
| Operations and Maintenance | 1,330,443 | 1,206,726 | 1,132,496 | 1,154,808 | 1,138,417 |
| Operations and Maintenance Navy Reserve | 75,781 | 77,166 | 78,788 | 77,187 | 78,503 |
| Military Personnel | 260,928 | 273,388 | 282,476 | 290,810 | 269,204 |
| **Total** | **$3,500,713** | **$3,017,617** | **$2,969,586** | **$2,883,737** | **2,937,084** |

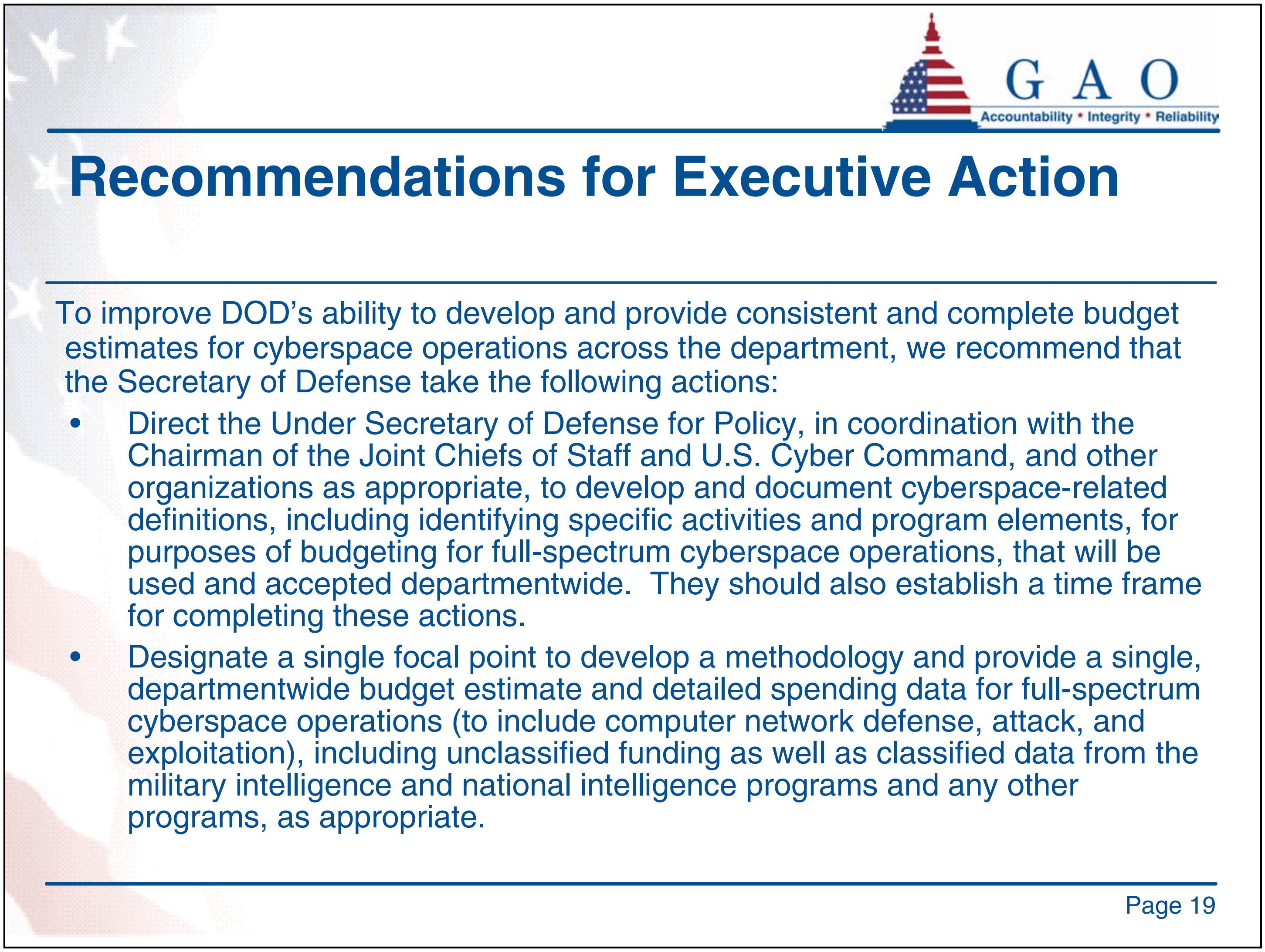
Note: Numbers do not include full-spectrum cyber operations.

Source: U.S. Navy.



# Conclusion

- DOD has taken many important steps to better organize its cyberspace efforts within a fairly short period of time. Without a complete budget estimate for full-spectrum cyberspace operations though, DOD and Congress do not have a complete picture of the resources DOD is investing in its cyberspace operations. We recognize that such challenges can occur as new mission areas are established. However, until DOD can provide a complete budget estimate for these operations, it will be difficult for the department and Congress to obtain an accurate and comprehensive view of the resources devoted to this emerging warfighting domain and make investment trade-off decisions. In light of the need to confront this serious national security threat and the fiscal constraints the nation is facing, it is important that DOD have better visibility of its cyberspace resources so that the department and Congress may prioritize among the program investments needed to defend DOD computer networks.



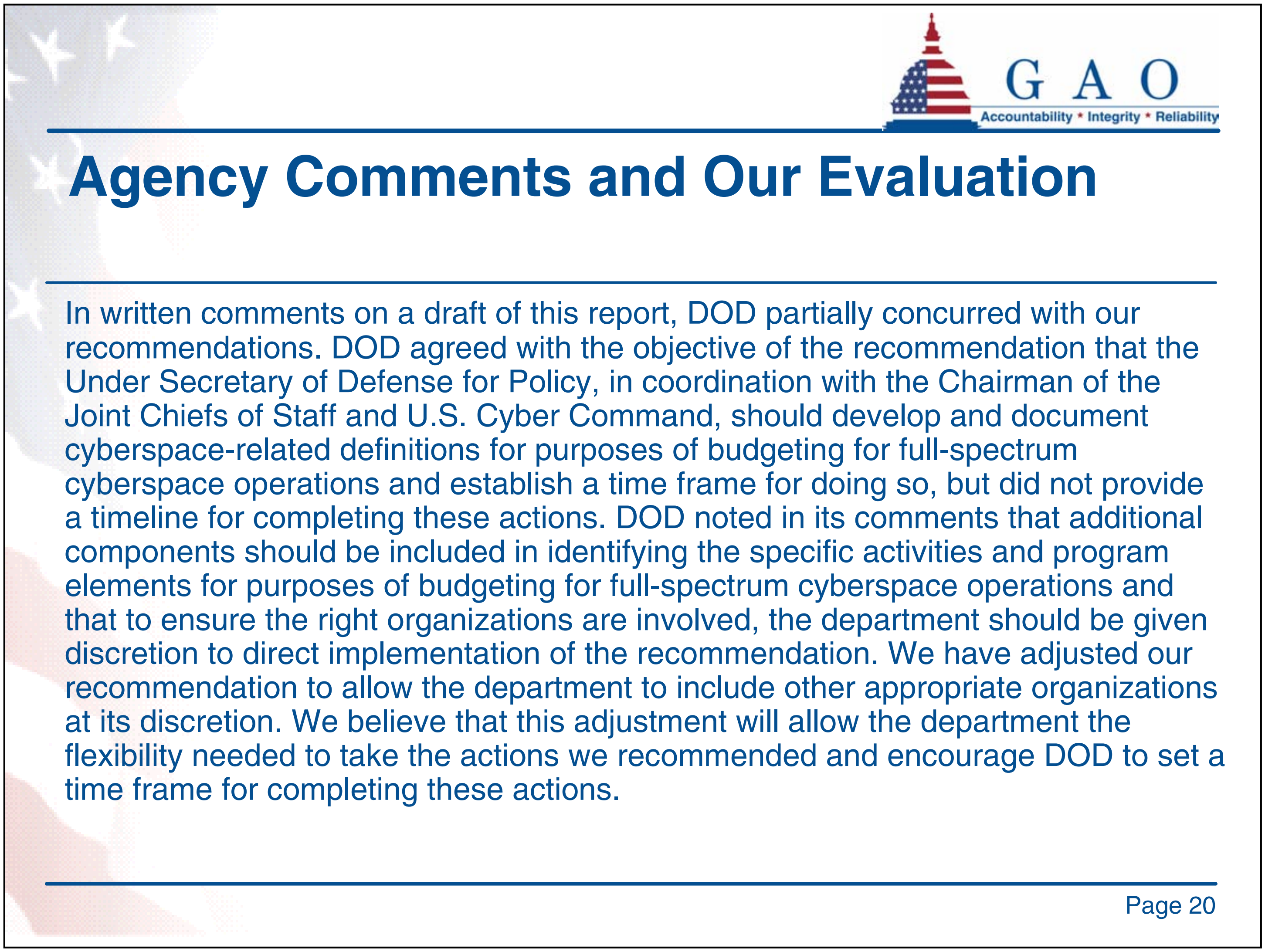
GAO
Accountability * Integrity * Reliability

## Recommendations for Executive Action

To improve DOD’s ability to develop and provide consistent and complete budget estimates for cyberspace operations across the department, we recommend that the Secretary of Defense take the following actions:

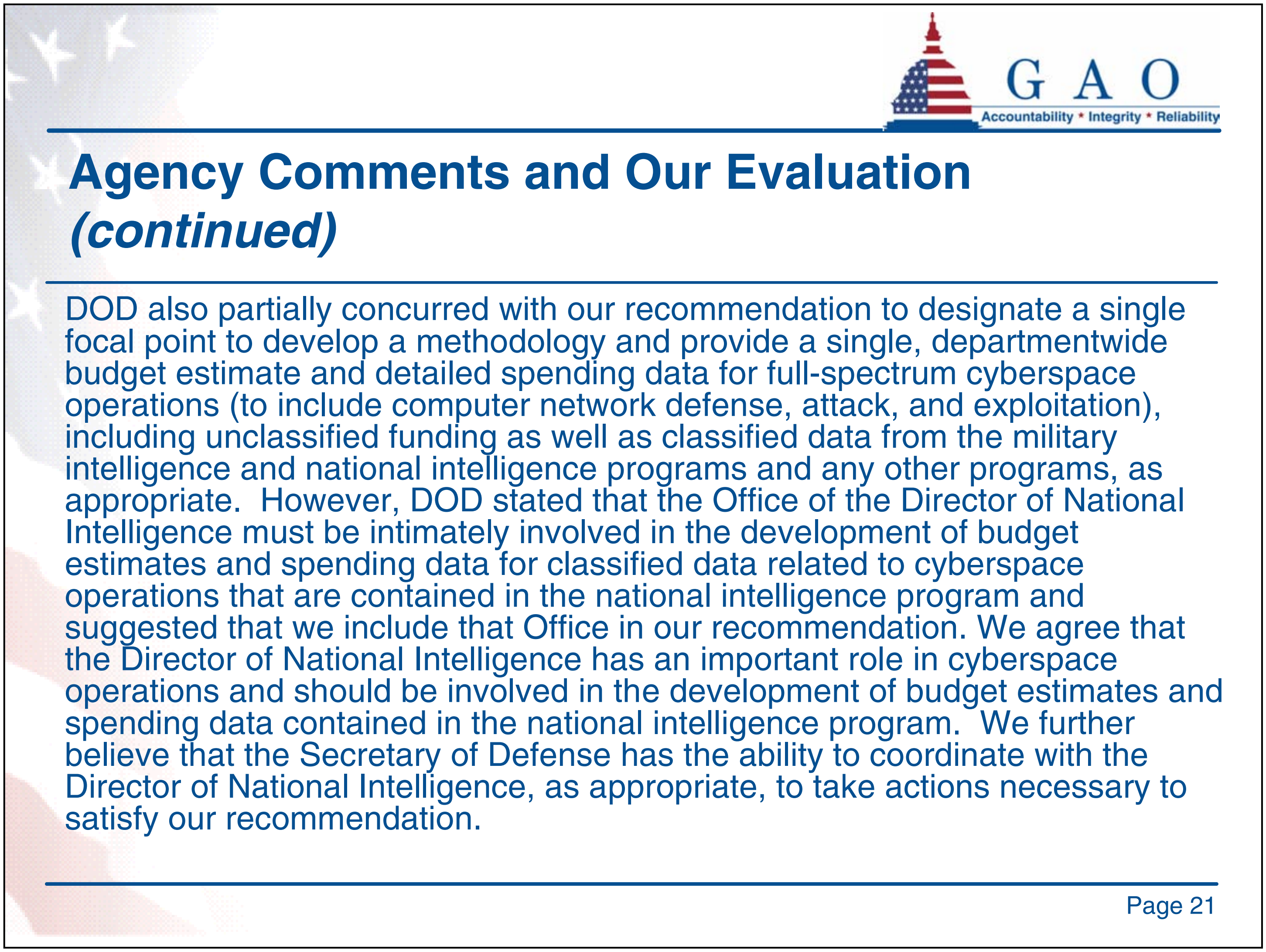
- Direct the Under Secretary of Defense for Policy, in coordination with the Chairman of the Joint Chiefs of Staff and U.S. Cyber Command, and other organizations as appropriate, to develop and document cyberspace-related definitions, including identifying specific activities and program elements, for purposes of budgeting for full-spectrum cyberspace operations, that will be used and accepted departmentwide. They should also establish a time frame for completing these actions.
- Designate a single focal point to develop a methodology and provide a single, departmentwide budget estimate and detailed spending data for full-spectrum cyberspace operations (to include computer network defense, attack, and exploitation), including unclassified funding as well as classified data from the military intelligence and national intelligence programs and any other programs, as appropriate.

Page 19



# Agency Comments and Our Evaluation

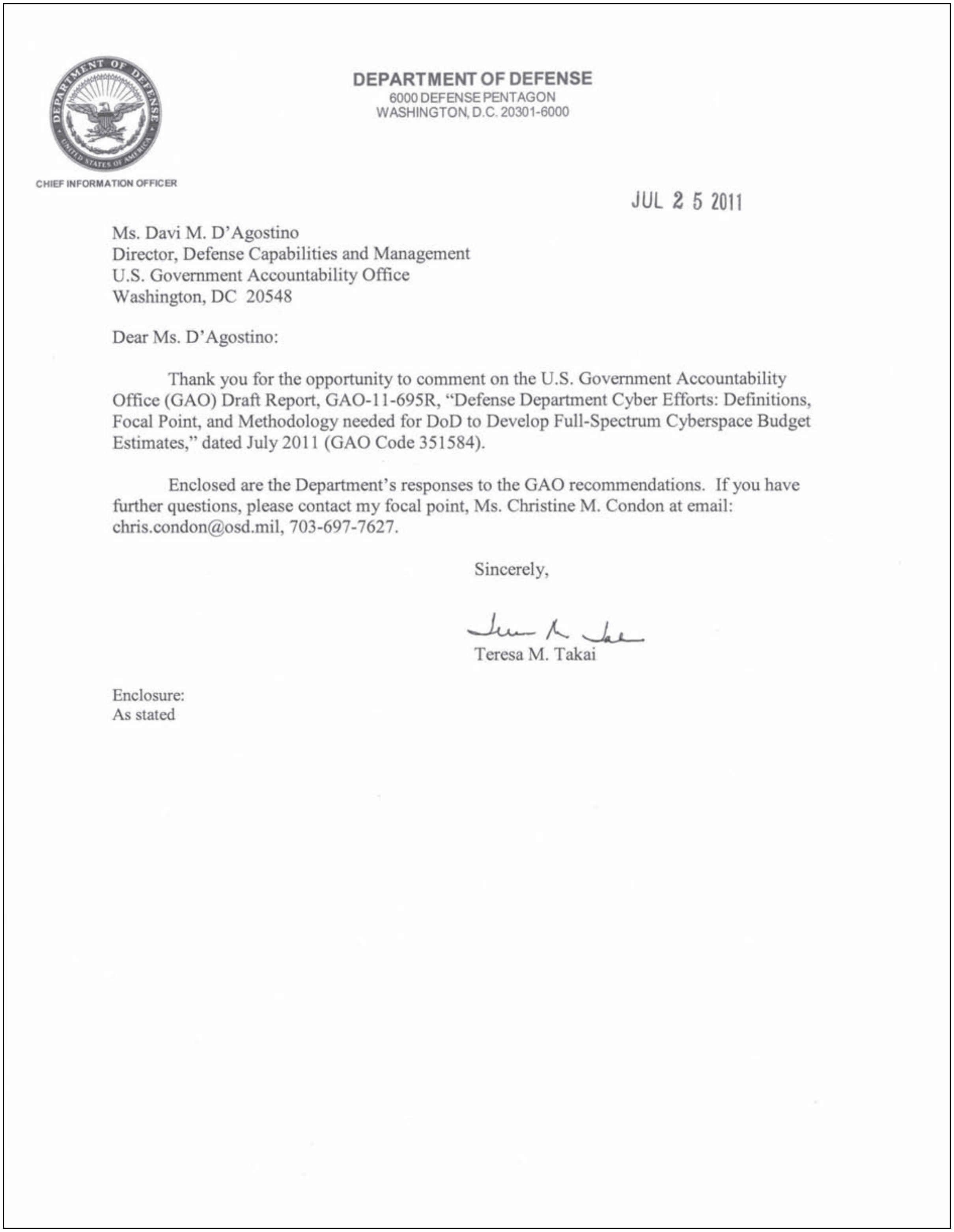
In written comments on a draft of this report, DOD partially concurred with our recommendations. DOD agreed with the objective of the recommendation that the Under Secretary of Defense for Policy, in coordination with the Chairman of the Joint Chiefs of Staff and U.S. Cyber Command, should develop and document cyberspace-related definitions for purposes of budgeting for full-spectrum cyberspace operations and establish a time frame for doing so, but did not provide a timeline for completing these actions. DOD noted in its comments that additional components should be included in identifying the specific activities and program elements for purposes of budgeting for full-spectrum cyberspace operations and that to ensure the right organizations are involved, the department should be given discretion to direct implementation of the recommendation. We have adjusted our recommendation to allow the department to include other appropriate organizations at its discretion. We believe that this adjustment will allow the department the flexibility needed to take the actions we recommended and encourage DOD to set a time frame for completing these actions.



## Agency Comments and Our Evaluation *(continued)*

DOD also partially concurred with our recommendation to designate a single focal point to develop a methodology and provide a single, departmentwide budget estimate and detailed spending data for full-spectrum cyberspace operations (to include computer network defense, attack, and exploitation), including unclassified funding as well as classified data from the military intelligence and national intelligence programs and any other programs, as appropriate. However, DOD stated that the Office of the Director of National Intelligence must be intimately involved in the development of budget estimates and spending data for classified data related to cyberspace operations that are contained in the national intelligence program and suggested that we include that Office in our recommendation. We agree that the Director of National Intelligence has an important role in cyberspace operations and should be involved in the development of budget estimates and spending data contained in the national intelligence program. We further believe that the Secretary of Defense has the ability to coordinate with the Director of National Intelligence, as appropriate, to take actions necessary to satisfy our recommendation.

Enclosure II



DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

CHIEF INFORMATION OFFICER

JUL 2 5 2011

Ms. Davi M. D'Agostino
Director, Defense Capabilities and Management
U.S. Government Accountability Office
Washington, DC 20548

Dear Ms. D'Agostino:

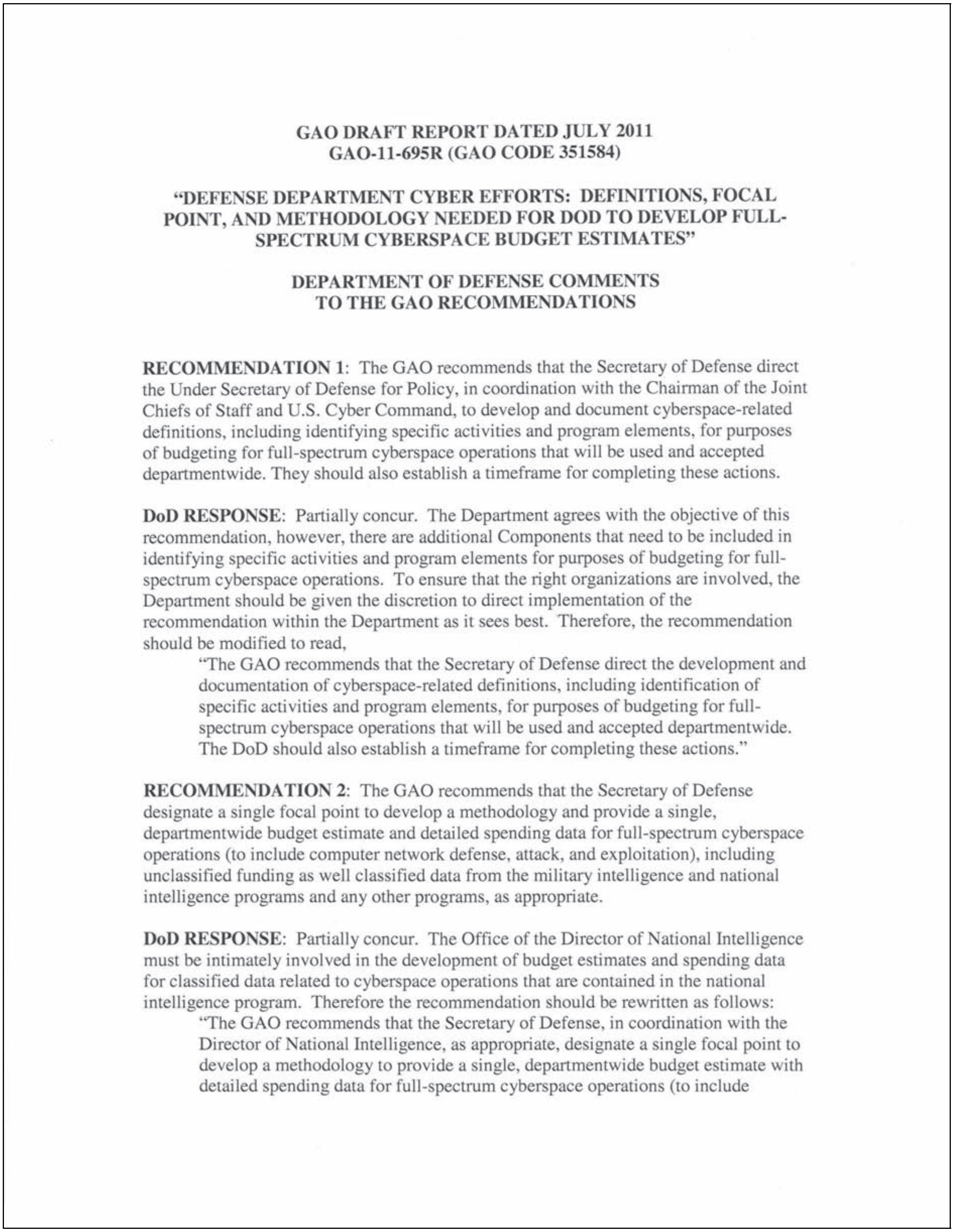
Thank you for the opportunity to comment on the U.S. Government Accountability Office (GAO) Draft Report, GAO-11-695R, "Defense Department Cyber Efforts: Definitions, Focal Point, and Methodology needed for DoD to Develop Full-Spectrum Cyberspace Budget Estimates," dated July 2011 (GAO Code 351584).

Enclosed are the Department's responses to the GAO recommendations. If you have further questions, please contact my focal point, Ms. Christine M. Condon at email: chris.condon@osd.mil, 703-697-7627.

Sincerely,

Teresa M. Takai

Enclosure:
As stated



**GAO DRAFT REPORT DATED JULY 2011**
**GAO-11-695R (GAO CODE 351584)**

**"DEFENSE DEPARTMENT CYBER EFFORTS: DEFINITIONS, FOCAL POINT, AND METHODOLOGY NEEDED FOR DOD TO DEVELOP FULL-SPECTRUM CYBERSPACE BUDGET ESTIMATES"**

**DEPARTMENT OF DEFENSE COMMENTS**
**TO THE GAO RECOMMENDATIONS**

**RECOMMENDATION 1**: The GAO recommends that the Secretary of Defense direct the Under Secretary of Defense for Policy, in coordination with the Chairman of the Joint Chiefs of Staff and U.S. Cyber Command, to develop and document cyberspace-related definitions, including identifying specific activities and program elements, for purposes of budgeting for full-spectrum cyberspace operations that will be used and accepted departmentwide. They should also establish a timeframe for completing these actions.

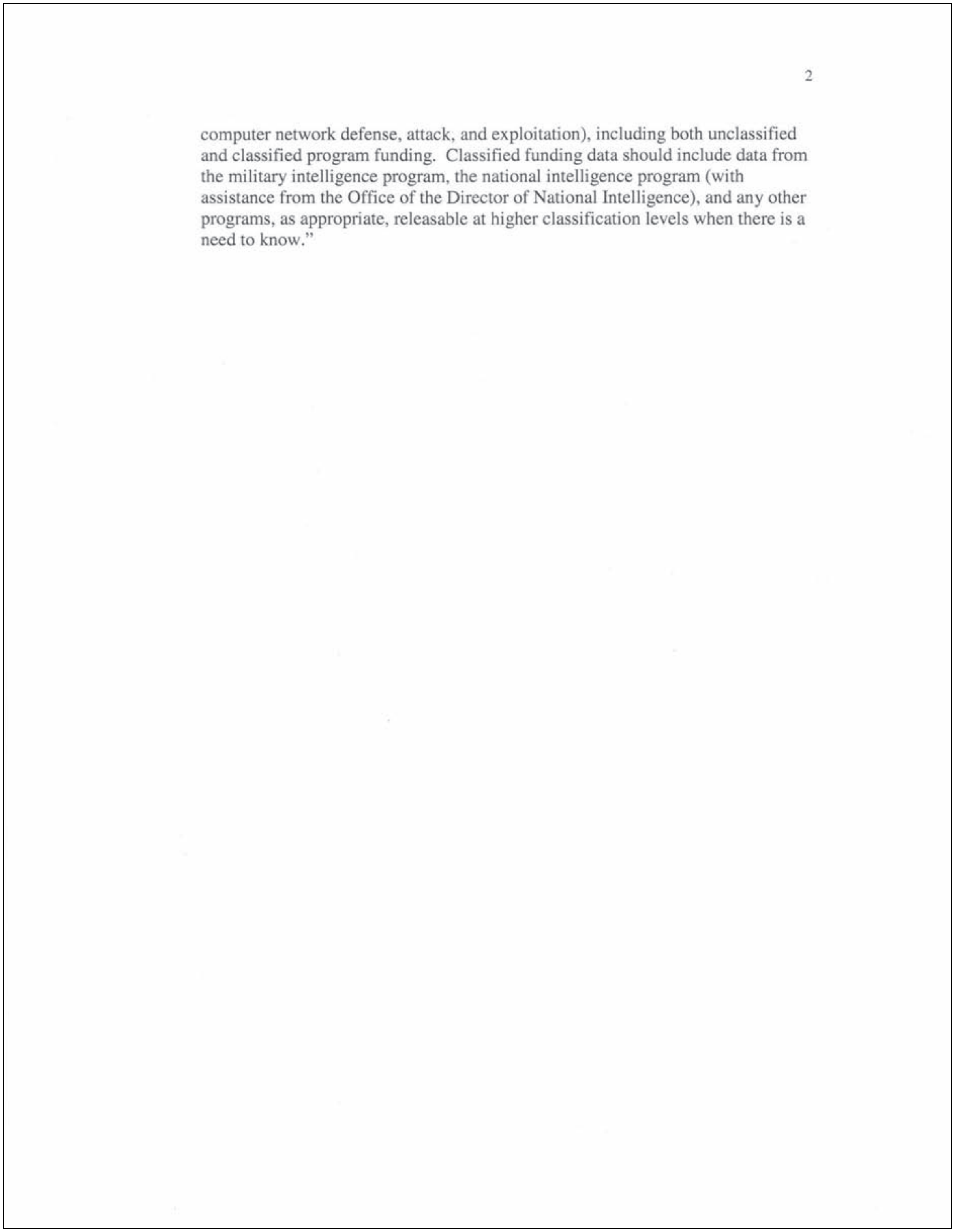
**DoD RESPONSE**: Partially concur. The Department agrees with the objective of this recommendation, however, there are additional Components that need to be included in identifying specific activities and program elements for purposes of budgeting for full-spectrum cyberspace operations. To ensure that the right organizations are involved, the Department should be given the discretion to direct implementation of the recommendation within the Department as it sees best. Therefore, the recommendation should be modified to read,

> "The GAO recommends that the Secretary of Defense direct the development and documentation of cyberspace-related definitions, including identification of specific activities and program elements, for purposes of budgeting for full-spectrum cyberspace operations that will be used and accepted departmentwide. The DoD should also establish a timeframe for completing these actions."

**RECOMMENDATION 2**: The GAO recommends that the Secretary of Defense designate a single focal point to develop a methodology and provide a single, departmentwide budget estimate and detailed spending data for full-spectrum cyberspace operations (to include computer network defense, attack, and exploitation), including unclassified funding as well classified data from the military intelligence and national intelligence programs and any other programs, as appropriate.

**DoD RESPONSE**: Partially concur. The Office of the Director of National Intelligence must be intimately involved in the development of budget estimates and spending data for classified data related to cyberspace operations that are contained in the national intelligence program. Therefore the recommendation should be rewritten as follows:

> "The GAO recommends that the Secretary of Defense, in coordination with the Director of National Intelligence, as appropriate, designate a single focal point to develop a methodology to provide a single, departmentwide budget estimate with detailed spending data for full-spectrum cyberspace operations (to include



computer network defense, attack, and exploitation), including both unclassified and classified program funding. Classified funding data should include data from the military intelligence program, the national intelligence program (with assistance from the Office of the Director of National Intelligence), and any other programs, as appropriate, releasable at higher classification levels when there is a need to know."

## GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

## Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

### Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or
TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

## Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

## Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548